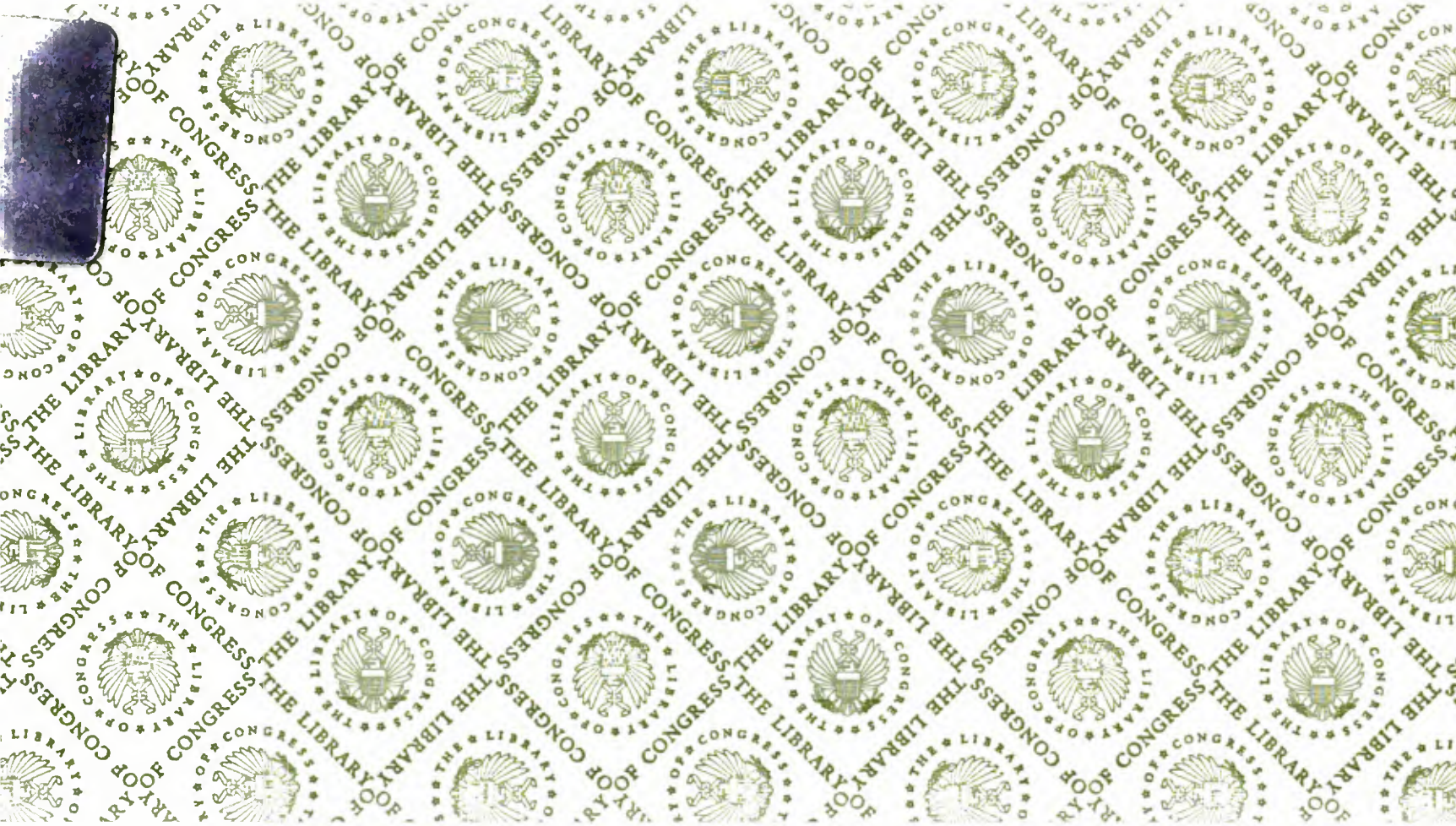
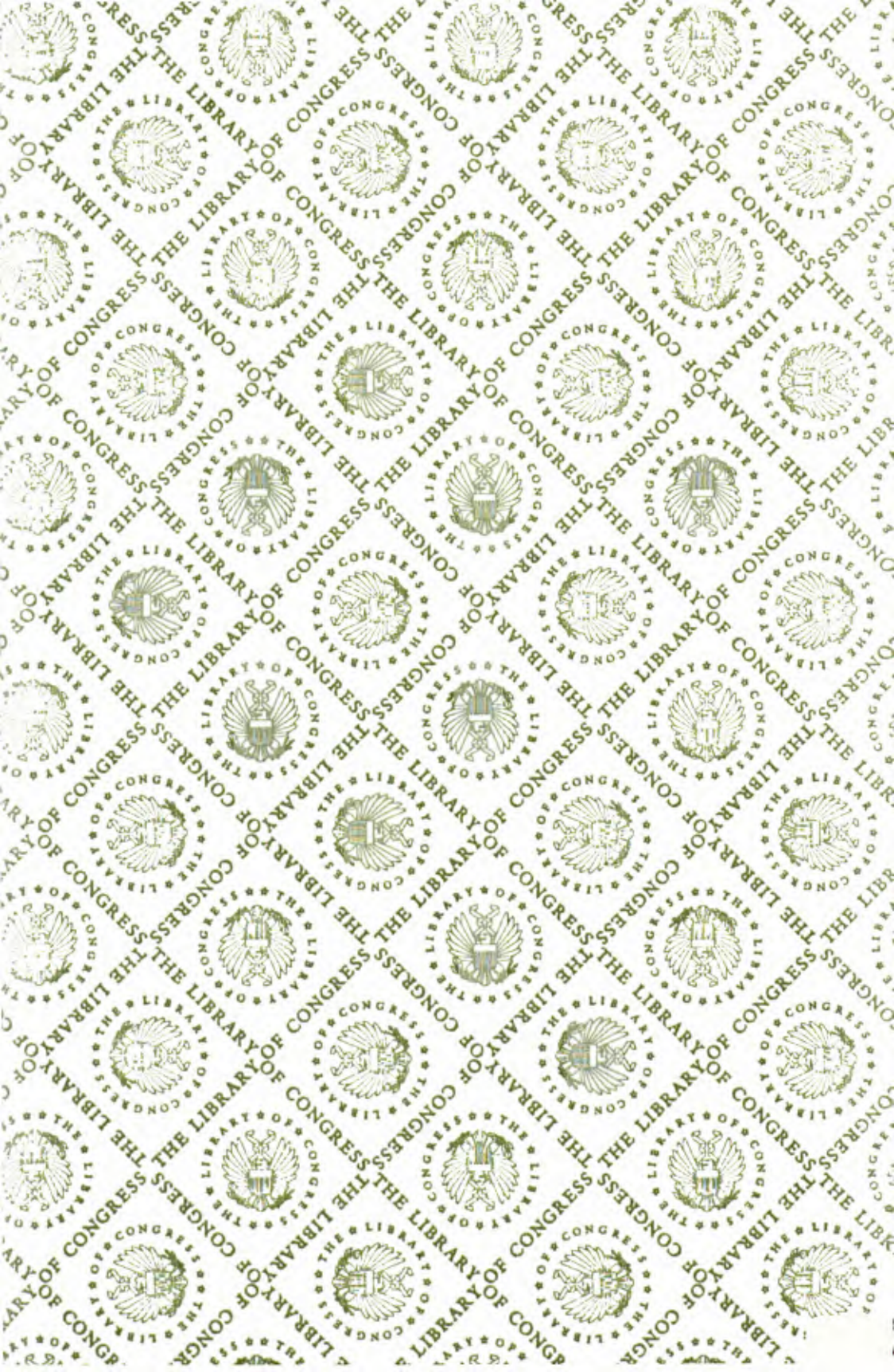

THE LIBRARY OF CONGRESS


THE LIBRARY OF CONGRESS

# ELECTRONIC COMMUNICATION PRIVACY POLICY DISCLOSURE



# HEARING

BEFORE THE

## SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

OF THE

## COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

MAY 27, 1999

**Serial No. 55**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
62-502 WASHINGTON : 2000

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-060799-X

## COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR S. SMITH, Texas
ELTON GALLEGLY, California
CHARLES T. CANADY, Florida
BOB GOODLATTE, Virginia
ED BRYANT, Tennessee
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
EDWARD A. PEASE, Indiana
CHRIS CANNON, Utah
JAMES E. ROGAN, California
LINDSEY O. GRAHAM, South Carolina
MARY BONO, California
SPENCER BACHUS, Alabama
JOE SCARBOROUGH, Florida

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York

THOMAS E. MOONEY, SR., *General Counsel-Chief of Staff*
JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

---

## SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

HOWARD COBLE, North Carolina, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
WILLIAM L. JENKINS, Tennessee
EDWARD A. PEASE, Indiana
CHRIS CANNON, Utah
JAMES E. ROGAN, California
MARY BONO, California

HOWARD L. BERMAN, California
JOHN CONYERS, JR., Michigan
RICK BOUCHER, Virginia
ZOE LOFGREN, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida

MITCH GLAZIER, *Chief Counsel*
BLAINE MERRITT, *Counsel*
VINCE GARLOCK, *Counsel*
DEBBIE K. LAMAN, *Counsel*
ROBERT RABEN, *Minority Counsel*
EUNICE GOLDRING, *Staff Assistant*

# CONTENTS

## HEARING DATE



## OPENING STATEMENT



## WITNESSES



## LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING



## APPENDIX

# ELECTRONIC COMMUNICATION PRIVACY POLICY DISCLOSURE

THURSDAY, MAY 27, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS AND
INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The subcommittee met, pursuant to call, at 10 a.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble [chairman of the subcommittee] presiding.

Present: Representatives Howard Coble, Bob Goodlatte, Edward A. Pease, Chris Cannon, Howard L. Berman, Zoe Lofgren and William D. Delahunt.

Staff present: Blaine Merritt, Counsel; Mitch Glazier, Chief Counsel; Eunice Goldring, Staff Assistant; and Bari Schwartz, Minority Counsel.

## OPENING STATEMENT OF CHAIRMAN COBLE

Mr. COBLE. Good morning, ladies and gentlemen. Welcome. The subcommittee will come to order.

Collecting demographic data, such as a consumer's address and telephone number, has become an important function of any business wishing to track customers and their habits. With the advent of the Internet as a medium for commercial transactions, the ability to acquire such information in exacting detail has been greatly enhanced. This development has also enabled businesses to take marketing strategies and offer those products and services which their customers truly want.

On the other hand, some critics believe that these gains have been offset by what they claim are the invasive nature of industry practices. They believe that greater efforts must be made to afford individuals better control of the subsequent use of any personal information collected by businesses with websites.

The purpose of this oversight hearing is to explore the tension between these two positions. In effect, this will be a state-of-the-industry examination of on-line privacy disclosure.

Mr. Berman will join us imminently. But I want to extend special thanks to the gentleman from Roanoke Valley, Mr. Goodlatte, who is here, for his leadership on this issue. He has a special interest in privacy disclosure. I welcome his input today as well as that of Mr. Berman, the ranking member, the gentleman from California.

Now we have a journal vote, but prior to going into a rest period, Mr. Goodlatte, would you like to be heard?

Mr. GOODLATTE. Mr. Chairman, thank you very much. I do have a statement that I will ask to be made a part of the record, and I will offer part of it right now.

I very much appreciate your holding this very timely and important hearing. The issue of privacy and security of personal information on the Internet is growing more important every day.

As consumers continue to look to the Internet more and more for commercial, financial, and business activities, the need for adequate privacy protections also continues to increase. On-line sales over the Christmas holiday last year topped $3 billion, Internet sales for all of last year topped $32 billion, and the numbers this year are expected to be even more impressive.

Nevertheless, these numbers represent only a fraction of the level of electronic commerce activity that could be realized if consumers' concerns about on-line privacy are addressed. Consumers have a fear of the Internet because they perceive that personal information, whether it is an address, phone number, credit card number, credit report or medical history, is not protected on the Internet.

Recent high-profile stories involving the release of sensitive consumer information on-line confirmed this in consumers' minds. Until consumers begin to have confidence that their information is protected from fraud or abuse, the Internet as a mode of commercial activity will not reach its full potential.

There are several laws currently on the books today designed to protect consumer information both on-line and off-line. These include the Electronic Communications Privacy Act, the Fair Credit Reporting Act, the Right to Financial Privacy Act and the Health Insurance Portability and Accountability Act.

In addition, several laws have been passed specifically to address the privacy of information involving certain advanced technologies, including the Cable Communications Policy Act, the Telephone Consumer Protection Act, and the Electronic Funds Transfer Act. Most recently, Congress passed the Children's On-line Privacy Protection Act, which directs the FTC to develop regulations governing the on-line collection of information from children under the age of 13.

However, general privacy protections for consumer information on-line have not been addressed by Congress. This Congress, and myself in particular, have been reluctant to pass sweeping laws that place undue restrictions on Internet activity.

The Internet is, at its core, an open medium that has succeeded because of its lack of control by any single entity, whether government or private sector. In fact, I have sponsored several pieces of legislation that would reduce or remove the government from involvement in various on-line activities.

In addition, the private sector has taken a number of steps to address this perceived deficiency in privacy on-line. Many businesses have formed alliances for the purpose of creating and administering several regulatory programs.

Some of these associations include the Online Privacy Alliance, representing more than 70 global companies concerned with on-line

privacy; TRUSTe, a collaboration between the Electronic Frontier Foundation and Commerce Net; and the newly developed Internet Fraud Council, designed to develop tools and best practices to be used to alleviate the threat of on-line crime to their members and to the general public. Industry has also developed tools to encourage website operators to educate consumers about the privacy policies for their site.

Most recently, a study conducted by a Georgetown University professor at the request at the Federal Trade Commission demonstrated significant improvement in the use of disclosure policies that include one or more of the five core FTC privacy principles: notice, consent, access, security and enforcement.

Specifically, 93 percent of those commercial websites sampled collected at least one type of personal identifying information, 53 percent collected at least one type of demographic information, and 56 percent collected both types of information. Of those sampled, 66 percent posted at least some kind of privacy disclosure; that is, some kind of privacy policy notice or an information practice statement.

Of the top 100 websites, 94 percent posted at least——

Mr. COBLE. Would the gentleman suspend for just a moment. How long is your statement?

Mr. GOODLATTE. Just about 30 more seconds, Mr. Chairman.

Mr. COBLE. All right.

Mr. GOODLATTE. The number of sites that provide consumers with the type of notice required by Online Privacy Alliance, the Better Business Bureau and TRUSTe and called for by the Federal Trade Commission remains around 10 percent of all commercial websites.

The Federal Government is no better. A study by the Center for Democracy and Technology of Federal agency websites found that just over 30 percent of Federal agencies had a privacy notice link from the agency's home page.

The private sector has made significant gains in the area of consumer privacy protection, but they must not be allowed to rest on their laurels. More must be done to ensure that the Internet is a medium that consumers can use with confidence, that their information is protected from fraud and abuse. I am hopeful that this hearing today will not only examine what has been accomplished but also examine what else needs to be done in the area of on-line privacy.

Mr. Chairman, I thank you for your forbearance.

Mr. COBLE. I thank the gentleman.

[The prepared statement of Mr. Goodlatte follows:]

PREPARED STATEMENT OF HON. BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Thank you, Mr. Chairman, for holding this timely and important hearing this morning. The issue of privacy and security of personal information on the Internet is growing more important every day. As consumers continue to look to the Internet more and more for commercial, financial, and business activities, the need for adequate privacy protections also continues to increase. Online sales over the Christmas holiday last year topped $3 billion. Internet sales for all of last year topped $32 billion, and the numbers this year are expected to be equally impressive. Nevertheless, these numbers represent only a fraction of the level of e-commerce activity that could be realized if consumers' concerns about online privacy are addressed.

Consumers have a fear of the Internet because they perceive that personal information, whether it is an address, phone number, credit card number, credit report, or medical history, is not protected on the Internet. Recent high-profile stories involving the release of sensitive consumer information online confirm this in consumers' minds. Until consumers begin to have confidence that their information is protected from abuse or fraud, the Internet as a mode of commercial activity will not reach its full potential.

There are several laws currently on the books today designed to protect consumer information, both online and offline. These include the Electronic Communications Privacy Act, the Fair Credit Reporting Act, the Right to Financial Privacy Act, and the Health Insurance Portability and Accountability Act. In addition, several laws have been passed specifically to address the privacy of information involving certain advanced technologies, including the Cable Communications Policy Act, the Telephone Consumer Protection Act, and the Electronic Funds Transfer Act. Most recently, Congress passed the Children's Online Privacy Protection Act, which directs the FTC to develop regulations governing the online collection of information from children under the age of 13.

However, general privacy protections for consumer information online have not been addressed by Congress. This Congress, and myself in particular, has been reluctant to pass sweeping laws that place undue restrictions on Internet activity. The Internet at its core is an open medium that has succeeded because of a lack of control by any single entity, whether government or private sector. In fact, I have sponsored several pieces of legislation that wold reduce or remove the government from regulating in various online activities.

In addition, the private sector has taken a number of steps to address the perceived deficiency in online privacy. Many businesses have formed alliances for the purpose of creating and administering self-regulatory programs. Some of these associations include the Online Privacy Alliance, representing more than 70 global companies concerned with online privacy, TrustE, a collaboration between the Electronic Frontier Foundation and CommerceNet, and the newly developed Internet Fraud Council, designed to develop tools and best practices to be used to alleviate the threat of online crime to their members and to the general public.

Industry has also developed tools to encourage website operators to educate consumers about the privacy policies for that site. This posting of privacy policies on commercial websites can empower consumers to make educated choices about whether they wish to deal with the particular merchant based, in part, on the level of privacy protection the online operator provides.

Most recently, a study conducted by a Georgetown University professor at the request of the Federal Trade Commission demonstrated significant improvement in the use of disclosure policies that included one or more of the five "core" FTC privacy principles: notice, consent, access, security, and enforcement. Specifically, 93 percent of those commercial websites sampled collected at least one type of "personal identifying" information, 53 percent collected at least one type of "demographic information," and 56 percent collected both types of information.

Of those sampled sites, 66 percent posted at least one kind of "privacy disclosure"—that is, some kind of privacy policy notice or an information practice statement. Of the top 100 commercial websites, 94 percent posted at least one type of privacy disclosure. While these statistics reflect significant improvement on the part of online commercial websites, the amount of information disclosed to consumers remains inconsistent. The number of sites that provide consumers with the types of notices required by the Online Privacy Alliance, the Better Business Bureau, and TrustE and called for by the Federal Trade Commission remains around 10 percent of all commercial websites.

The Federal government is no better. A study by the Center for Democracy and Technology of federal agency websites found that just over 30 percent of federal agencies had a "privacy notice" link from the agency's home page.

The private sector has made significant gains in the area of consumer privacy protection, but they must not be allowed to rest on their laurels. More must be done to ensure that the Internet is a medium that consumers can use with the confidence that their information is protected from fraud and abuse. I am hopeful that this hearing today will not only examine what has been accomplished, but also what remains to be done in the area of online privacy. I thank the Chairman for holding this hearing this morning, and I look forward to hearing from our witnesses. Thank you.

Mr. COBLE. We will suspend for the moment, go vote; and I have a markup in transportation. Mr. Goodlatte, will you be able to assume the chair?

Mr. GOODLATTE. I will.

Mr. COBLE. And I will be back and forth.

We have two panels today. Good to have all of you with us. We will return imminently.

[Recess.]

Mr. GOODLATTE. [Presiding.] The subcommittee will reconvene.

At this time, the chair is pleased to recognize the ranking member, Mr. Berman of California.

Mr. BERMAN. Thank you very much, Mr. Chairman. I appreciate your consideration.

I have to go to International Relations in a little while, so I would like to give the statement and then come back to hear as much of the witnesses' testimony as I can.

I think it is an excellent idea that you and Chairman Coble are holding this hearing. This is a very important social issue, and I think it falls right within the jurisdiction of our subcommittee.

Every day millions log on to the Internet and provide personal information—age, gender, address, phone number, marital status, credit card and even very personal family, medical and financial information and much other information—to public and private organizations from whom they want information or a service or to owners of websites that they are simply interested in exploring.

Every day millions undertake Internet searches and create a trail that, if followed, could reflect details about an individual's interests and often reveal facets of that individual's personality that few may know.

Every day millions provide personal information on the use of ATM and credit cards and through other electronic transactions. Some foresee a single card that carries our "personal identity" on it.

Financial, medical, government and other institutions that manage vast volumes of private information are finding new uses for this information.

As new means are developed to collect and manage personal information gathered through the Internet and other electronic means, the American public is becoming more aware of the potential uses and misuses for this personal information; and people are becoming more interested in finding ways to protect their privacy and control the use of information that they disclose and that which is captured as they navigate the electronic world.

Some testifying today will argue for legislation. Some will propose continued industry self-regulation as the solution. I will be interested in what everyone here has to say, and I will be listening with an awareness of the uniqueness of the Internet environment.

Some describe that environment as anarchic in nature, since anyone can maintain a website and can do so essentially without accountability, except to their conscience.

This is not to say that businesses cannot develop and adhere to good privacy policies, doing so would certainly be good business practice; and this is not to say that individuals using the Internet have no responsibility in protecting their own privacy, though we have to look hard at the environment that we are creating for this truly is a new world.

Personal information that was once unavailable de facto, just a simple mass of—the inaccessibility of it—an example being county property records gathering dust at the Recorders office—is now available in a keystroke.

Information that was one considered private has become a commodity to the bought, sold and traded.

Information that once we gave freely, knowing that the particular piece of information provided little insight into our life-styles, is now aggregated to reveal the patterns of our personal behavior.

Where once we would walk into a bookstore and pay cash for a book, remaining entirely anonymous, we now provide detailed information to benefit from the cost savings of buying on-line.

With this in mind, we must consider the current and potential effectiveness of self-regulation, including how self-regulation may work in the context of frequently changing business models, mergers and acquisitions.

And we need to consider the role of government in protecting the privacy interests of the individual.

Finally, I would like to note as we address privacy in electronic communications, it is among our responsibilities to consider whether current law is adequate to restrain the misuse of government-held private information in the modern electronic environment.

We are at a critical juncture where we must assess whether new laws are necessary to protect the right of individuals to privacy and whether industry is on the right track toward healthy self-regulation, and I look forward to hearing and reading the testimony from each of our witnesses today.

Thank you, Mr. Chairman.

Mr. GOODLATTE. I thank the gentleman.

Does the gentlewoman from California have any opening statement?

Ms. LOFGREN. No.

Mr. GOODLATTE. Thank you.

Well, we are very pleased to welcome the very patient Mr. John Bentivoglio—is that how you pronounce your name?

Mr. BENTIVOGLIO. Correct.

Mr. GOODLATTE [continuing]. Our government witness this morning, who is the Chief Privacy Officer for the Department of Justice.

The Chief Privacy Officer reports directly to the Attorney General and Deputy Attorney General on privacy policy matters and chairs the Department's Privacy Council. The Council serves as a clearinghouse for privacy-related legislative regulatory and policy initiatives, provides advice to senior Department officials on privacy matters and provides a forum for exchanging information about important developments in the field of privacy.

In addition, he serves as the Department's special counsel for health care fraud, where he is responsible for overseeing and coordinating the Department's health care fraud program, including civil and criminal enforcement matters and prevention and compliance efforts.

Mr. Bentivoglio received his undergraduate degree at the University of California-Berkley and his law degree from the Georgetown University Law School Center.

The subcommittee has copies of your testimony, which, without objection, will be made a part of the record; and we would welcome you. And please limit your oral statement to 5 minutes.

**STATEMENT OF JOHN BENTIVOGLIO, CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF JUSTICE**

Mr. BENTIVOGLIO. Thank you. Good morning, Mr. Goodlatte, Ms. Lofgren.

Mr. GOODLATTE. Chairman works while I am here.

Mr. BENTIVOGLIO. I am sorry.

I am John Bentivoglio, and I serve as the Chief Privacy Officer for the Department. In that job, I am responsible for coordinating the Department's efforts to protect individual privacy rights. I appreciate this opportunity to present the Department's views on the issue of electronic privacy disclosure practices.

Before I do so, however, I would like to briefly describe what the Department is doing to ensure we engage in appropriate privacy practices and set a good example for others in both the public and private sector.

Last year, as you noted, the Attorney General created the position of Chief Privacy Officer and established a Privacy Council within the Department. The Council, which I chair, is composed of senior officials from the FBI, DEA, the Criminal and Civil Divisions, and other key DOJ components. I should add that the Criminal Division and FBI are very strong supporters of the Council and participate in a very, very meaningful way; and we feel this is very important.

The Council is currently reviewing a number of important privacy issues, including the Department's compliance with the Privacy Act, the sharing of information among Federal, State and local law enforcement agencies, and the impact of new law enforcement technologies on individual privacy. I am also pleased to note that we have posted a privacy policy on the Department's website.

In addition, the Department has enacted internal policies and procedures to ensure strict adherence to communications privacy protections, and we have a record of aggressively pursuing violations of the Electronic Communications Privacy Act.

Turning to the primary subject of today's hearing, electronic privacy disclosure practices raise a host of important issues, including law enforcement issues of concern to the Department of Justice. There has been a great deal of discussion over public concern about the loss of on-line privacy and the adequacy of industry self-regulatory efforts with respect to the collection, use, and disclosure of personal information on-line.

We share these concerns. We believe, however, that industry has made substantial strides, as evidenced by the recent draft Georgetown Internet Privacy Policy Survey. As you know, that survey—based on a sample of more than 360 of the most popular websites—found that 65.7 percent—nearly two-thirds—of the sites surveyed—posted a privacy policy or an information practice statement.

Contrasted with the 14 percent rate of privacy policy disclosure found by the Federal Trade Commission's similar survey in 1988, the dramatic 1-year improvement reflects a determined effort on the part of industry to improve its information practices. This

progress follows calls by the President, Vice President and others for industry to lead the way in protecting on-line privacy, and many industry leaders, including the Online Privacy Alliance and its members, deserve recognition for their efforts.

While we are encouraged by these results, we would also point out another important finding of the Georgetown study. Less than 10 percent of the most frequently visited sites and less than 15 percent of the sites that collect personal information had a comprehensive privacy policy that includes a posted privacy policy and addresses five key principles of fair information practices—notice, choice, access, security and contact information.

Thus, while we are pleased at the significant progress made by industry in the past 12 months, we need the final third of websites to post privacy policies that adhere to all the principles of fair information practices.

Mr. Chairman, I think my statement goes into this at greater depth, but there is an important connection between on-line privacy and our efforts to fight fraud and other criminal conduct.

In closing, I want to reiterate the Department's commitment to furthering the administration's principles as outlined in the Framework for Global Electronic Commerce. The Framework urged a multipronged approach to privacy protection, relying on a combination of industry self-regulation, sector-specific legislation, and enforcement efforts to prevent unfair deceptive trade practices. In addition, the Department will vigorously enforce Federal laws designed to protect individual privacy, including the new identity theft statute.

We look forward to working with Congress and the private sector to achieve these goals.

Mr. GOODLATTE. Thank you very much.

[The prepared statement of Mr. Bentivoglio follows:]

PREPARED STATEMENT OF JOHN BENTIVOGLIO, CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF JUSTICE

My name is John Bentivoglio. I serve as the Chief Privacy Officer for the U.S. Department of Justice, where I am responsible for coordinating the Department's efforts to protect individual privacy rights. I appreciate this opportunity to present the Department's views on the issue of electronic privacy disclosure practices.

Before I do so, however, I would like to briefly describe what the Department of Justice (DOJ) is doing to ensure we, as a Department, engage in appropriate privacy practices and set a good example for others in both the public and private sector. Last year, the Attorney General created the position of Chief Privacy Officer and established a Privacy Council within the Department. The Council, which I chair, is composed of senior officials from the FBI, DEA, the Criminal and Civil Divisions, and other DOJ components. The Attorney General directed that the Council "serv[e] as a clearinghouse for privacy-related legislative, regulatory and policy initiatives, provid[e] advice to senior Department officials on privacy matters, and provid[e] a forum for exchanging information about important developments in the field of privacy." The Council is currently reviewing a number of important issues, including the Department's compliance with the federal Privacy Act; the sharing of information among federal, state, and local law enforcement agencies; and the impact of new law enforcement technology on individual privacy. I am also pleased to note that we have posted a privacy policy on the Department's web site.

In addition, the Department has enacted internal policies and procedures to ensure strict adherence to communications privacy protections and we have a record of aggressively pursuing violations of the Electronic Communications Privacy Act. That Act establishes a number of substantive and procedural safeguards on law enforcement access to electronic communications, which is sometimes required in the course of the investigation of federal crimes.

Turning to the primary subject of today's hearing, electronic privacy disclosure policies raise a host of important issues, including law enforcement issues of concern to the Department of Justice. There has been a great deal of discussion over public concern about the loss of online privacy and the adequacy of industry self-regulatory efforts with respect to the collection, use, and disclosure of personal information online. We share these concerns. We believe, however, that industry has made substantial strides, as evidenced by the recently reported results of the draft Georgetown Internet Privacy Policy Survey. As you know, that survey—based on a sample of more than 360 of the most popular web sites—found that 65.7%—nearly two thirds of the sites surveyed—posted a privacy policy or an information practice statement. Contrasted with the 14% rate of privacy policy disclosure found by the Federal Trade Commission's similar survey in 1998, the dramatic one-year improvement reflects a determined effort on the part of industry to improve its information practices. This progress follows calls by the President and Vice President for industry to lead the way in protecting online privacy, and many industry leaders, including the Online Privacy Alliance and its members, deserve special recognition for their efforts.

While we are encouraged by these results, we would also point out another important finding in the Georgetown study—less than 10 percent (9.4%) of the most frequently visited sites and less than 15 percent (14.7%) of the sites that collect personal information had a comprehensive privacy policy that includes a posted privacy policy and addresses five key principles of fair information practices—notice, choice, access, security, and contact information. Thus, while we are pleased at the significant progress made by industry in the past 12 months, we need the final third of web sites to post privacy policies that adhere to all the principles of fair information practices. Posting a privacy policy is an essential first step to protecting privacy in cyberspace, but to be effective, privacy policies must be ubiquitous and comprehensive. We believe more can and should be done by industry to safeguard the privacy of online consumers.

The Department strongly supports industry efforts to enhance and safeguard online privacy. In addition to protecting online privacy, the use of third-party certifications, such as those developed by TRUSTe, BBBOnline, and CPA Webtrust can help consumers avoid web sites that have inadequate privacy safeguards, including web sites operated by scam artists—a growing concern to the Department of Justice.

Although there are strong market incentives to develop privacy disclosure policies, and we support industry self-regulatory efforts, some practices involving the collection and use of personal information may run afoul of federal and state laws. Under the Federal Trade Commission Act, for example, the FTC may pursue injunctive relief against businesses whose information collection and use practices constitute an unfair or deceptive trade practice, such as the failure to comply with a web site's posted privacy policies. The FTC has brought enforcement actions in this area.

Although the Department of Justice has no authority to sanction businesses that fail to establish privacy disclosure policies, we are concerned about the interplay between online privacy and consumer fraud. The disclosure of personal information in the online environment may unwittingly expose individuals to a host of on- and offline dangers. For example, posting personal information in a chat room can expose a person to solicitations for fraudulent investments, electronic harassment or stalking (both on- and offline), and, in the case of minors, attempts to establish an illicit sexual relationship or contact. Since the Internet offers anonymity not available in the offline world, some individuals are not sufficiently aware of the dangers of disclosing sensitive information in the online environment. The Department has launched a number of initiatives to respond to these issues, including a new Internet Fraud Initiative, which is designed to increase federal prosecution of Internet fraud scams and to prevent such scams through consumer education and prevention.

We also are concerned about the growing problem of "identity theft," the use of another person's identifying information to commit an offense (such as using a Social Security number to obtain a credit card fraudulently). In some instances, this information is obtained without any contact with the victim of the fraud, such as when sham information brokers obtain personal financial information through pretext calls. In other instances, the information is obtained from the victim online when the perpetrator poses as a business person and gains the victim's trust through frequent and seemingly innocent communications. Armed with such information as a person's social security number, bank account information, and date of birth, scam artists have been stealing thousands of dollars from individual consumers—without any contact whatsoever with the victim. Last year, Congress enacted legislation aimed at this problem, and the Administration has announced an enforcement and prevention initiative that contemplates referral of cases among fed-

eral, state, and local law enforcement and regulatory agencies, and development of a private-public partnership to educate consumers on ways to protect themselves.

In addition, at our request, the U.S. Sentencing Commission amended its guidelines to allow for increased penalties for fraudulent offenses that involve a significant invasion of individual privacy. The Commission also is charged with amending the guidelines, as appropriate, to provide penalties for each offense under 18 U.S.C. § 1028, including the new identity theft statute. We hope the new statute and these enhanced penalties will serve as a deterrent to fraud artists who invade individual privacy in order to commit their scams.

Finally, we are working closely with the FTC and others to ensure aggressive enforcement of federal laws designed to protect individual privacy. For example, the Fair Credit Reporting Act provides criminal penalties for knowing and intentional violations of the Act. The FTC receives consumer complaints about potential violations of the Act and refers potential criminal violations to the Department for appropriate follow-up, and we are working with the FTC to better identify cases suitable for criminal prosecution.

Significantly, ubiquitous electronic privacy disclosure policies should help educate consumers about the dangers associated with the unguarded disclosure of sensitive personal information. If privacy disclosure policies and third-party privacy certifications become the norm, consumers may be more cautious about disclosing personal information to web sites that may not be privacy sensitive or are merely electronic fronts for scam artists. In educating consumers about online personal privacy, and in promoting informed disclosure by consumers based on individual choice, such private-public partnerships will also serve to inform Internet users about the potential risks of unguarded disclosure of personal information. In sum, our hope is that enhanced public awareness, brought about in part through the educational efforts of the private sector, will promote responsible decision-making among Internet users about when and to whom to disclose personal information, thereby reducing harassment and misuse.

In closing, I want to reiterate the Department's commitment to furthering the Administration's principles as outlined in the Framework for Global Electronic Commerce in July 1997. The Framework urged a multi-pronged approach to privacy protection, relying on a combination of industry self-regulation, sector-specific legislation (as for fraudulent "pretext calls" used by unscrupulous data brokers to obtain private financial records), and enforcement efforts to prevent unfair or deceptive trade practices. In addition, the Department will vigorously enforce federal laws designed in whole or in part to protect individual privacy, including the new identity theft statute.

We look forward to working with Congress and private industry to achieve these goals. I would be happy to answer any questions you might have.

Mr. GOODLATTE. I wonder if you might comment in some detail about how well the Electronic Communications Privacy Act is combating privacy violations and fraudulent activity.

Mr. BENTIVOGLIO. Well, we think ECPA, as it is referred to, is doing a good job in that sense. It includes strong protections, including criminal penalties for violations of communication privacy rules.

We have brought a number of factors for violations of ECPA. One important factor, though, is that the public is not always aware of violations of ECPA and thus they don't bring those to our attention. So we don't really know how serious the problem is because many people don't know that it is being violated. When they do, they bring them to our attention; and we pursue them very vigorously.

Mr. GOODLATTE. Are there any ongoing efforts to make the public aware of their rights under that law?

Mr. BENTIVOGLIO. We have engaged industry very aggressively in this regard, and that is because industry would probably know earlier than others about potential violations. If someone is hacking, industry might know that, private sector communications providers might know that and bring that to our attention. That is an important source of referrals.

But we do try to engage others and use various public forums to highlight those protections so that people will bring them to our attention.

Mr. GOODLATTE. But you find that that law is an effective tool for law enforcement in helping to reduce fraud in electronic communications?

Mr. BENTIVOGLIO. It is one of the tools we use, yes.

Mr. GOODLATTE. Okay. Is there a need for laws like ECPA to address the fact that, even though there are many, many dedicated folks in industry who are attempting to combat fraud through self-regulation, you are always going to have some bad actors out there who want to carve out a niche for themselves, where they are going to benefit by the fact that everyone else is complying with the law and they are going to try to slip under the radar screen, if you will?

Mr. BENTIVOGLIO. We don't believe that legislation is necessary at this time.

Mr. GOODLATTE. No, but I am talking about ECPA.

Mr. BENTIVOGLIO. I don't think that we foresee changes necessarily to ECPA.

Mr. GOODLATTE. No, no, no, that is not what I am referring to. I am saying legislation like ECPA is helpful in ferreting out the bad actors that you deal with on a regular basis.

Mr. BENTIVOGLIO. ECPA is helpful in that regard, yes.

Mr. GOODLATTE. Good. Good.

Those are all the questions I have. Ms. Lofgren.

Ms. LOFGREN. Just a few.

On page 5 of your testimony, you discuss the Justice Department's initiatives including the Internet Fraud Initiative Against Scams. We all agree that is important. How many prosecutions have occurred in the course of this fraud initiative?

Mr. BENTIVOGLIO. The initiative was just announced approximately 2 weeks ago by the President, so there have been no prosecutions since that time. We have brought prosecutions against Internet fraud scams, although this is a relatively new area, and so the number would not be that great.

Ms. LOFGREN. How many agents and U.S. Attorneys are assigned or intended to be involved in this prosecutorial activity and where are they assigned?

Mr. BENTIVOGLIO. Right now, we are working with the FBI, the Fraud Section in the Criminal Division and the U.S. Attorneys to get this initiative under way and implemented. I don't know the specific numbers. But, for example, we have computer and telecommunications coordinators in every U.S. Attorney's Office. They are a resource for these types of cases, as are white-collar-crime prosecutors. So all the U.S. Attorney's Offices will be engaged to some extent in this initiative.

Ms. LOFGREN. Well, without mentioning any office, some offices have more depth in this area than others and some offices have virtually no capacity in terms of who happens to be there as an attorney to deal with these types of matters. What systematic effort is under way to upgrade the skillset in offices where that is the case?

Mr. BENTIVOGLIO. Well, you highlight an important issue, which is the training and expertise of our agents and prosecutors. These days not only do you need to be a good lawyer, you need to be very

knowledgeable about technology and communications issues and the like. We have taken a number of steps in that regard.

First, in every U.S. Attorney's Office, as I mentioned, there is a computer and telecommunications coordinator, a CTC. They receive extensive training from the Computer Crime Section and the Criminal Division on these type of issues. So every U.S. Attorney's Office has some expertise and depth in this area.

We also have training programs—local, regional and national training programs to boost the training and expertise of our prosecutors and investigators. The investigative side is very important. And the FBI has invested a lot of resources and energy—those resources, of course, provided by Congress—to this effort. So there is a steep learning curve here.

I can't say that we have done everything—I can't say that we have the expertise that we are comfortable with, but we are working very diligently in that regard.

Ms. LOFGREN. I don't know whether you can discuss in depth the FBI. But, as one example, there recently was a change in Silicon Valley. The FBI disbanded its high-tech unit. We found this very mysterious—especially in Silicon Valley. The unit has recently been reformatted somehow—although not as a separate unit.

When I looked at expertise, I looked at some of the prosecutions we've had and the training level in two various FBI offices. I find it is all over the board. It really does seem to be fortuitous. There are some officers that have computers at home, learn about computers and know about it. Other officers think that a mouse is an animal with a tail. It doesn't seem to be a cohesive effort on the part of the Bureau. Is there something more systematic under way—other than having an officer who is supposed to be in charge? Unless there's more, it is really not going to translate out to the troops in terms of putting a case together?

Mr. BENTIVOGLIO. There is a very systematic effort under way within the Bureau to develop the expertise and the capability in the computer crime area, and I think it would be probably easiest to provide details for the record and to you on that issue. But I know that the Bureau is very, very committed to this issue. They do have rigorous training efforts under way. And their CART teams, which are in various offices around the country, are some of the most sophisticated computer crime experts anywhere in the world.

Ms. LOFGREN. Don't misunderstand me. The Bureau has excellent people: I don't mean to suggest otherwise. But it is a bit spotty.

If I could, Mr. Chairman. I realize my light is on. Could I ask one more question? Thank you.

On page 6, you talk about stealing identification information, and the like. How many prosecutions have occurred in this arena? What kind of forces are deployed in this effort?

Mr. BENTIVOGLIO. I am not aware of any prosecutions since that new statute has passed. We have prosecuted identity theft under prior statutes, mail and wire fraud statutes. That statute was passed late last year. It has been approximately 6 months. I believe we have some investigations under way. I don't think there have been any prosecutions.

I can say that the FBI is working with the Secret Service, which has jurisdiction over this as well, and they have a number of ongoing investigations under way. And they are working very closely together to share information, to make sure we are diligently pursuing that statute.

Ms. LOFGREN. Okay. Thank you, Mr. Chairman.

Mr. GOODLATTE. Mr. Bentivoglio, I wonder if you might comment on some of the types of fraud that you have encountered on-line.

Mr. BENTIVOGLIO. They range in complexity from very simple scams where legitimate-appearing websites will offer certain services—that if you provide a credit card number, they will provide certain services, and then the credit card number is provided on-line. The account is billed, and then no services are rendered.

Mr. GOODLATTE. Have you prosecuted anybody under those types of scams?

Mr. BENTIVOGLIO. I believe we have.

There are also more sophisticated scams, and those scams also could be prosecuted by State district attorneys' offices, depending on where the people are and the like. And in some cases where the dollar amounts are low, we might refer those for handling by State and local authorities.

On the other hand, there have been sophisticated securities fraud scams which we are working with the SEC in pursuing. Those are more sophisticated scams, targeted at many investors, some of them whom are very sophisticated, who have been scammed by these fraud artists.

Mr. GOODLATTE. Now, if these website operators were to fully disclose what their purpose is in gathering information, some of these instances of fraud would be reduced, would they not?

Mr. BENTIVOGLIO. Not necessarily. Sometimes you can disclose a privacy policy, and then the policy can be a complete sham. We think privacy policies help us on the fraud front, primarily by educating consumers about the need to be cautious about the information that they do provide. You can post a seal or you can create the appearance of a seal that gives the appearance of legitimacy. Yet it could be just a fraudulent site. So that alone won't stop them.

But really the consumers are the first line of defense here, and the more they know about the dangers of providing information on-line and how to do it safely, the less fraud there will be.

Mr. GOODLATTE. If they give the appearance of protecting somebody's privacy by posting a fraudulent policy, does that give you any additional remedies that you can take against them in terms of criminal prosecution?

Mr. BENTIVOGLIO. Like under the mail and wire fraud statute, there has to be a scheme or an artifice to defraud primarily for financial gain. So if they just fail to post a privacy policy or didn't comply with it but there was no further scheme or artifice to defraud, we probably would not have jurisdiction to pursue them criminally. Although, in that sense, criminal prosecution might be too much in that regard; a regulatory action or a civil action may be the appropriate approach.

If there is financial gain, though, that would tend to fall within the mail and wire fraud statutes; and we would probably go after that.

Mr. GOODLATTE. Most of the industry folks represented here today I think are very conscious and aware of this and are participating in these various programs I have described to give adequate information, adequate notice to consumers about what may be used with information. But what do you do with the person who is using the information they gather for a legal purpose? They are not committing credit card fraud or something like that. They are simply going to legally sell information they gather to somebody else who may use it for some purpose that the consumer, not being aware of that fact, may not want their particular information used for that purpose. What do you do about those kinds of circumstances where there is no disclosure?

Mr. BENTIVOGLIO. Under the fact pattern you described, we wouldn't have jurisdiction to pursue that.

Mr. GOODLATTE. Do you have a concern about that type of problem?

Mr. BENTIVOGLIO. We do. I know the Federal Trade Commission might have jurisdiction in that regard as that practice could, depending on the facts, constitute an unfair deceptive trade practice. They might have jurisdiction there.

I think we are concerned generally because of the connection to fraud and also because we think, you know, the high level of consumer concern about this is something we should take seriously. On the other hand, we don't have the authority to pursue that type of action.

Mr. GOODLATTE. But in order to deal with those portions of the website operators who are not participating voluntarily in these types of things and who are engaged in what otherwise would be perfectly legal uses of these things, in order for you to help that, you would need to have legislative authority, is that not right?

Mr. BENTIVOGLIO. That is correct.

Mr. GOODLATTE. Okay. She obviously doesn't have any other questions. I would very much like to thank you for your participation today.

And at this time we will move on to our next panel, and we look forward to continuing to work with the Justice Department as this issue evolves. It is one that has a great deal of ramifications, and we want to proceed with a good deal of caution and with as much encouragement of the industry to take care of this problem as we possibly can.

Mr. BENTIVOGLIO. Thank you, Mr. Chairman.

Mr. GOODLATTE. So thank you.

We now invite our next panel.

Our first witness is Christine Varney, who is chair of the Online Privacy Alliance. Mrs. Varney has lectured extensively both in the United States and abroad on various legal issues in American politics. Ms. Varney's postgraduate degrees include a 1986 JD from Georgetown University Law Center, and a 1978 master's in public administration from the Maxwell School at Syracuse University. She attended Trinity College in Dublin, Ireland, and is a 1977 graduate of the State University of New York in Albany.

Ms. Varney is a member of the District of Columbia Bar, the New York State Bar, the American Bar Association and the National Lawyers Counsel.

Next, we will be hearing from Mr. Terry Pittman, who was elected to the Board of Directors for TRUSTe, a privacy initiative designed to stimulate the growth of electronic commerce by building consumer trust and confidence in the Internet and shape public policy regarding website's disclosure of individuals' personal and private information.

Mr. Pittman received his AB in 1980 from the University of North Carolina at Chapel Hill School of Journalism and mass communication.

Third, we will hear from Jerry Cerasale—am I right? I am two for two—who is Senior Vice President of Government Affairs at the Direct Marketing Association, who is in charge of the DMA's contact with the Congress, all Federal agencies and State and local governments.

Prior to joining the DMA, he was the Deputy General Counsel for the Committee on Post Office and Civil Service at the U.S. House of Representatives. He served for 12 years at the Postal Rate Commission as legal advisor to Chairman Steiger and most recently special assistant to the Commission. He received his BA in government and economics from Wesleyan University, Middletown, Connecticut, and his JD from the University of Virginia School of Law.

Next, we will hear from Jill Lesser, who is Vice President of Domestic Public Policy at America Online in Dulles, Virginia. She leads the company on domestic public policy, regulatory and industry relations activities and heads the Washington, D.C., office. At America Online, Ms. Lesser has led industrywide efforts on a number of emerging public policy issues effecting the Internet and the new information society.

Ms. Lesser earned her BA with honors in political science from the University of Michigan in 1987 and a JD from Boston University School of Law.

Then we will hear from Mark Rotenberg, Executive Director of the Electronic Privacy Information Center here in Washington, a public interest research organization working to protect privacy, free speech and constitutional values in the on-line world. Mr. Rotenberg is also an adjunct professor at Georgetown University Law Center, where he has taught the Law of Information Privacy since 1990, and a senior lecturer Washington College of Law.

He is a graduate of Harvard College and Stanford Law School.

And then last, but certainly not least, we will hear from Jerry Berman, President of the Center for Democracy and Technology. The Center was founded in December 1994 by Mr. Berman. Mr. Berman coordinates CDT's free speech and privacy policy working groups comprised of communications firms, associations and civil liberties groups which address Internet policy issues. He also chairs the Advisory Committee to the Congressional Internet Caucus, of which I am co-chairman.

Mr. Berman received his BA, MA and LLB from the University of California at Berkley.

Mr. GOODLATTE. We are pleased to start with Ms. Varney.

**STATEMENT OF CHRISTINE VARNEY, CHAIR, ONLINE PRIVACY ALLIANCE**

Ms. VARNEY. Thank you. Good morning, Mr. Chairman and members of the subcommittee. I would like to talk with you this morning about the efforts of industry to create a trusted on-line environment that respects individual privacy.

On behalf of the Online Privacy Alliance, a coalition of more than 80 companies and associations committed to consumer privacy, I would like to thank Dr. Mary Culnan of Georgetown University and the FTC for the excellent work done on the Georgetown Internet privacy study. The study has shed a great deal of life on the status of on-line privacy and provided guidance for our future efforts; and there will be future efforts, but a great deal remains to be done.

First, let us look at what has already been accomplished. In 1998, the Federal Trade Commission found that only 14 percent of websites had posted privacy policies. Although the Georgetown study survey sampled differed from last year's, the progress is indisputable. This year, in a sample drawn from the net's most popular sites, a remarkable 66 percent of sites had posted privacy policies. The astonishing leap to 66 percent shows that privacy on-line is becoming the standard.

This progress is largely the result of the partnership between the private sector working together with government, both the Congress and the executive branch, to make privacy the norm; and the progress has been just as notable among the top 100 most popular websites, 94 percent of which now have posted a privacy disclosure. This is up from 71 percent last year. These are the sites that consumers most often visit.

The unduplicated reach of the top 100 sites is about 94 percent, while the reach of the larger sample is about 98.8 percent. Consumers can now look for privacy policy at every website where they plan to transact business. They can refuse to do business with sites that don't have a policy; and they can, and should, send E-mail to websites without privacy policies asking or demanding that the site post one.

The Georgetown survey, while providing evidence of significant progress, also pointed out where more work needs to be done. The study showed the differences in the quality of privacy policies. The study showed that fewer than 15 percent of sampled sites included all the elements necessary for an acceptable privacy policy, including disclosure, choice, access and security.

The OPA also requires websites to provide contact information so consumers can get in touch with someone at a company when they have a privacy concern.

The Georgetown findings showed that the percentage of websites providing notice and disclosure is quite high, 87 percent of the sites surveyed; and the study found 77 percent of websites provide consumers with choice about how their personal information is used.

We believe that the 46 percent in the survey posting security precautions may not reflect the actual practice. It is likely that many sites which do indeed appropriately safeguard personal information are not clearly disclosing their security precautions in the privacy policy. This is not necessarily a problem of security but cer-

tainly a problem of communication. It needs to be fixed, and we intend to help do that.

Nevertheless, more work needs to be done to make privacy policy across the net meet basic standards for informing consumers about the policies and practices of on-line businesses. The policies must be easy to find, read, and understand.

The Online Privacy Alliance will work in the coming year to increase the number of websites posting privacy policies, and we will work to make sure the privacy policies give consumers the information they need to make informed decisions. We believe we can reach the skull through the enforcement of existing law and the industry promotion of best practices. Consumers who have the information they need to make informed choices are the best enforcers of privacy on-line.

Consumers must also take some responsibility and look for privacy policies, read them and make the choices. They must remember on the digital street as on the Main Street, think before you share information.

Thank you very much.

Mr. GOODLATTE. Thank you.

[The prepared statement of Ms. Varney follows:]

PREPARED STATEMENT OF CHRISTINE VARNEY, CHAIR, ONLINE PRIVACY ALLIANCE

The Internet is poised to become an explosive economic growth opportunity that will redefine global commerce in the information age. That growth cannot and will not occur without consumer confidence. Privacy is one of the cornerstones of consumer confidence in the Internet.

Last year numerous companies and associations came together to create policies and practices that can make privacy a reality for everyone on the Internet. These companies and associations, the Online Privacy Alliance, are pleased to submit the attached documents. First is the Mission Statement describing the goals of the Online Privacy Alliance, second are the Guidelines for Privacy Policies that will be adopted by all Online Privacy Alliance members, third are the Principles for Children's Online Activities, and fourth are the Guidelines for Effective Enforcement of Self-Regulation.

The Online Privacy Alliance has worked diligently to come up with policies that can be applied across many industry sectors. These guidelines, principles and statements reflect not only a deep commitment to online privacy, but also new policies which the Online Privacy Alliance members support. First, the Online Privacy Alliance believes that when there is use or distribution of individually identifiable information for purposes unrelated to that for which it was collected, individuals should be given the opportunity to opt out of such unrelated use or distribution. Second, the Online Privacy Alliance members believe that sites targeted at children under 13 should not engage in the collection and maintenance of information from children without prior parental consent. Finally, the Online Privacy Alliance members believe that self-regulation requires robust enforcement and they are committed to ensuring such.

Over the past year the OPA has worked to expand the adoption of effective online privacy policies by organizations doing business online. Clearly, the recent Georgetown Internet Privacy Policy Study ("the Georgetown Privacy Study") indicates that significant progress has been made in safeguarding privacy online. The fact that close to 66 percent of sites in the sample posted a privacy disclosure demonstrates that adoption and disclosure of privacy policies is becoming the norm on the Internet. Last year, the FTC reported that only 14 percent of Web sites notified consumers about their privacy policies. Although the universe from which the survey samples are drawn differ, it is very clear that there has been enormous progress.

The OPA and its supporting organizations will continue to work to ensure that effective online privacy practices are adopted and implemented among the private sector. In particular, we will be focusing on continuing outreach through business and consumer education, while increasing awareness of various privacy assurance programs. The Georgetown Privacy Study will serve as a road map to help us ensure that robust privacy practices are the norm online. It has been a pleasure work-

ing with this group and I look forward to continuing to work with the Online Privacy Alliance to build consumer confidence in the Internet.

Note: Additional materials supplied by Ms. Varney on Online Privacy Alliance (www.privacyalliance.org) are in the subcommittee's files.

Mr. GOODLATTE. Mr. Pittman.

## STATEMENT OF TERRY PITTMAN, BOARD OF DIRECTORS, TRUSTE

Mr. PITTMAN. Thank you very much, ladies and gentlemen of the committee.

Let me just add that, in addition to my role as a director at TRUSTe, I am an executive in a California Silicon Valley start-up and have spent the last 4 years in that space.

I would like to thank you first for inviting TRUSTe to testify on the very important issue of Internet privacy. For the past 2 years, TRUSTe's mission has been to increase trust on the Internet by promoting responsible and fair information collection and use practices on-line. TRUSTe's privacy program is based on the fair information practices called for by the Federal Trade Commission. Since the inception of our program in 1997, all TRUSTe licensees must post a privacy statement in a prominent location that fully discloses information collection and use practices.

In October 1998, TRUSTe introduced several additional elements to our program. All licensees must now provide a mechanism for consumers to update or correct personal information; provide an opportunity for users to opt-out of secondary use of their personal information; take reasonable security precautions to protect information that is collected; and, last, follow the requirements of the TRUSTe Children's Program, when the licensed website is targeted to children under the age of 13.

The cornerstone of TRUSTe's program is our verification and oversight. TRUSTe performs periodic reviews of each website to ensure compliance with TRUSTe requirements. TRUSTe also tracks usage of personal identifiers or personal information in the licensee's database, a process known as seeding. Seeding involves visiting and registering with the website under an assumed identity and then tracking how that information is used.

TRUSTe's consumer complaint resolution process, also known as our escalation process, begins if TRUSTe believes a licensee is in noncompliance of their stated privacy practices or if a consumer files a complaint through TRUSTe's watchdog site. If the investigation reveals that a site has violated its privacy statement, TRUSTe will require remedial measures. To assure that problems have been corrected, the site may be asked to undergo a—third party—audit. If the problem is not resolved through TRUSTe's satisfaction, we may revoke the TRUSTe sale, also called a trustmark. If an egregious or malicious privacy breach has occurred, the site may be referred to an appropriate local law enforcement agency or to the FTC.

As of today, TRUSTe has more than 675 licensed sites, those sites accounting for ⅓ of all U.S. Internet traffic. TRUSTe anticipates more than 1,500 sites will join the TRUSTe program by December 1999.

TRUSTe's growth is a result of aggressive business-to-business outreach. When we launched the TRUSTe seal program in June 1997, we understood that educating the most visible sites would be the key to the widespread adoption of privacy protection practices on the web.

Of particular note is that all major portal sites have joined TRUSTe, including America Online, Excite, Infoseek, Lycos, Microsoft, Netscape, Snap, and Yahoo. Forty-five of the top 100 sites are TRUSTe licensees. What is more, 80 percent of our licensed sites are small businesses.

As we move into the third year of our program, we are noticing a new trend. That is, traditional off-line brands, such as major manufacturers and Fortune 100 companies, are entering the TRUSTe program with greater and greater frequency.

The growth of interest in seal programs is clearly linked to one factor, the desire to build a web environment that consumers feel comfortable in. To that end, it has been TRUSTe's mission to provide outreach and education to web users about how to take control of their information on-line.

TRUSTe's grass-roots privacy partnership education campaign was the largest ever on-line public service announcement initiative. In a span of just 3 weeks, 200 million donated banner advertisements ran on the most visited U.S. websites. More than 1 million web users visited the educational campaign website to learn more about protecting their privacy. The campaign was a huge success.

I would like to spend a moment now briefly commenting on the results of the web survey completed recently by Mary Culnan of Georgetown University.

Mr. GOODLATTE. If you could do it briefly, we would appreciate it.

Mr. PITTMAN. Okay. I will wrap up.

When the program was launched 2 years ago, one of our most significant changes was to convince Web site owners that privacy was an important part of their activities. Now with 65.7 percent of commercial websites addressing the consumer privacy issue, we believe it is a remarkable demonstration; and that message has been received and acted on.

Finally, I would like to comment that we are launching programs around the globe with our European interim director; and we have ongoing discussions with agencies in Singapore, Australia and other countries who are interested in launching local TRUSTe programs there.

I would like to thank you for your invitation to speak here and look forward to serving as a resource for the committee and the House. Thanks.

Mr. GOODLATTE. Thank you.

[The prepared statement of Mr. Pittman follows:]

PREPARED STATEMENT OF TERRY PITTMAN, BOARD OF DIRECTORS, TRUSTE

Ladies and Gentlemen of the Committee:

I would like to thank you for inviting TRUSTe to testify on the very important issue of Internet privacy. For the past two years, TRUSTe's mission has been to increase trust on the Internet by promoting responsible and fair information collection and use practices online. TRUSTe's privacy program is based on the fair information practices called for by the Federal Trade Commission. Since the inception of our pro-

gram in 1997, all TRUSTe licensees must post a privacy statement in a prominent location that fully discloses information collection and use practices.

In October 1998, TRUSTe introduced several additional features to our program. All licensees must now:

- Provide a mechanism for consumers to update or correct personal information;
- Provide an opportunity for users to opt-out of secondary use of their personal information;
- Take reasonable security precautions to protect information that is collected; and
- Follow the requirements of the TRUSTe Children's Program when the licensed Web site is targeted to children under the age of 13.

The cornerstone of TRUSTe's program is our verification and oversight. TRUSTe performs periodic reviews of each site to ensure compliance with TRUSTe requirements. TRUSTe also tracks usage of unique identifiers in a licensee's database, a process we call seeding. Seeding involves visiting and registering with the Web site under an assumed identity, then tracking how that registration information is used.

TRUSTe's consumer complaint resolution process, also known as our escalation process, begins if TRUSTe believes a licensee is in non-compliance of stated privacy practices or if a consumer files a complaint through TRUSTe's watchdog site. If an investigation reveals that a site has violated its privacy statement, TRUSTe will require remedial measures. To assure that problems have been corrected, the site may be asked to undergo a third-party audit. If the problem is not resolved to TRUSTe's satisfaction, we may revoke the TRUSTe seal, also called a trustmark. If an egregious or malicious privacy breach has occurred, the site may be referred to an appropriate local law enforcement agency, or to the Federal Trade Commission.

As of today, TRUSTe has more than 675 licensed sites; those sites account for one-third of all US Web traffic. TRUSTe anticipates that more than 1,500 sites will join its privacy oversight program by December 1999.

TRUSTe's growth is a result of aggressive business-to-business outreach. When we launched the TRUSTe seal program in June of 1997, we understood that educating the most visible sites would be key to the widespread adoption of privacy protection practices on the Web.

Of particular note is that all major Internet "portal" sites have joined TRUSTe, including America Online, Excite, Infoseek, Lycos, Microsoft, Netscape, Snap, and Yahoo! 45 of the top 100 sites are TRUSTe licensees. What's more, 80% of our licensed sites are small businesses. As we move into the third year of our program, we are noticing a new trend. Traditional "off-line" brands, such as major manufacturers and Fortune 100 companies, are entering the TRUSTe program with greater and greater frequency.

The growth of interest in seal programs is clearly linked to one factor: the desire to build a Web environment that consumers feel comfortable in. To that end, it has also been TRUSTe's mission to provide outreach and education to Web users about how to take control of their information online. TRUSTe's grass-roots Privacy Partnership education campaign was the largest ever online public service announcement initiative. In a span of 3 weeks, 200 million donated banner advertisements ran on the most trafficked U.S. Web sites. More than one million Web users visited the educational campaign Web site to learn more about protecting their privacy. The campaign was a huge success, with more than 800 Web sites joining in to run banner ads.

I would like to spend a moment now commenting on the results of the survey of Web sites recently completed by Mary Culnan of Georgetown University. When TRUSTe launched, nearly two years ago, one of our most significant challenges was to convince Web site owners that privacy was an issue they should put resources toward. The fact that now, 65.7% of commercial Web sites are addressing consumer privacy is a remarkable demonstration that the message has been received, loud and clear.

Now that two-thirds of all sites are posting some type of privacy notice, the mission of seal programs is clear—evangelize the need for comprehensive statements that address all fair information practices. Seal programs offer turn-key solutions to sites by ensuring they adhere to all fair information practices prior to granting the seal.

Finally, I would like to mention that TRUSTe was launched with the intent of creating a globally recognized seal program. Already, we have licensees in English-speaking countries around the world. This year, we launched our European program by appointing an interim European director. We have ongoing discussions with

agencies in Singapore, Australia, and several other countries with an interest in launching the TRUSTe program locally. We will continue to keep you updated on these international efforts.

We thank you for the opportunity to speak here today and look forward to serving as a resource for the Judiciary Committee and all members of the House of Representatives.

Mr. GOODLATTE. Mr. Cerasale.

**STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.**

Mr. CERASALE. Thank you very much.

I appreciate the opportunity to testify here today on behalf of Direct Marketing Association and ask that my written testimony submitted for the record.

Mr. GOODLATTE. Without objection. In fact, all of your written testimony will be made a part of the record.

Mr. CERASALE. Thank you.

The Direct Marketing Association represents numerous companies that offer products to consumers through all types of media. The Internet is one that our companies are beginning to look at as a new way to reach customers, offer them products and goods at a reasonable price; and we depend upon consumer confidence and consumer trust in order to have these marketplace grow; and so it is very important for us to ensure that there is trust of the consumer in the marketplace.

We have taken a good deal of effort on a number of public education and technology and self-regulatory initiatives to advance privacy and consumer choice in the on-line environment.

We are very pleased with the results of the Georgetown study. It shows a significant improvement in posting of privacy policies on the net. But is the job done? It is not, as others have said here today. We have a long way to go. But we are on the right track, and that is the direction we are moving.

We have specifically supported and helped craft the Children's Privacy Protection Act, and we are now working with the Federal Trade Commission as we move forward with the regulations to implement that act and try to protect children in the use of their information on-line.

In the next 2 months, the Direct Marketing Association will implement two self-regulatory initiatives to try and further empower in the marketplace on-line. On July 1st, 1999, the DMA's privacy promise will become mandatory for all DMA members. Basically, that is in the on-line and the telephone and in the mail media. Companies will have to give notice of what they use—what information they collect and how they use it, whether they give it out to third parties and provide an opportunity for the consumer to say no. We think that that is a major push, and I think that is one area where we have to grow and continue our efforts, based upon the Georgetown study.

We are also developing an E-mail preference service, which would be a service that individuals can put their E-mail address on and our companies would have to not send an unsolicited E-mail message to them—very similar to our mail preference service and our telephone preference service.

We have been working with the worldwide web consortium to create a privacy policy tool to try and let the Internet be seamless in a privacy means, to allow a consumer to put his or her privacy policy on his or her browser, have the companies put their privacy policy on the front of their Web site. If there is a match, you go in; if not, there is some dialogue between the company and the consumer.

I think it is very important as we look at this Internet that there are many, many major technological tools that are being developed to try and help promote control of the consumer over information that he or she gives over the net.

We also believe that we are pushing hard now with TrustE, with BBB Online and other seal programs that will become more and more known to consumers on the Net, and that way self-regulation will be moving forward. We think it is very important that, with the Internet being borderless, we should be very careful to try not to overregulate it because our regulation may not be exactly what other countries will do, and we can very much tie up the Net and prevent the growth that we are all looking forward to.

Thank you very much.

[The prepared statement of Mr. Cerasale follows:]

PREPARED STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

SUMMARY

I am Senior Vice President of Government Affairs for The Direct Marketing Association, Inc ("The DMA"). The DMA is the largest trade association for businesses interested in direct, database, interactive marketing and electronic commerce. The DMA represents more than 4,500 companies in the United States and 54 other nations. Founded in 1917, its members include direct mailers and direct marketers from 50 different industry segments, as well as the non-profit sector. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet based businesses and a host of other segments, as well as the service industries that support them.

The DMA member companies have a major stake in the success of electronic commerce, and are among those most likely to benefit immediately from its growth. The DMA's leadership is continuing to extend into the Internet and electronic commerce areas with its recent acquisitions of the Internet Alliance and the Association for Interactive Media. Members of The DMA include L.L. Bean, Time Inc., Dell Computer, Gateway 2000, DoubleClick, autobytel.com, BMG Direct, Charles Schwab & Co., Lucent Technologies, eBay, Acxiom, AT&T, America Online, IBM, MCI WorldCom, and others. Accordingly, The DMA has been working diligently to apply its successful self-regulatory system from the traditional media to the Internet and its World Wide Web.

We have worked intensively on a number of public education, technology and self-regulatory initiatives that advance privacy and consumer choice in the online environment. Due in large part to the efforts of our members, self-regulation is working in the Internet context. Just last week this conclusion was reinforced with the release of the results of the Georgetown Internet Privacy Policy Study. This study demonstrates that significant progress has been made in safeguarding privacy online. In the past year, 66 percent of all sites surveyed posted privacy policies, a dramatic increase from the 14 percent rate shown by a study last year. Moreover, the study showed that 94 percent of the top 100 sites posted privacy policies.

In the next two months, The DMA will implement two self-regulatory initiatives that will further empower consumers and demonstrate the tenacity of industry in acting responsibly on this issue. First, on July 1, 1999, The DMA Privacy Promise goes into effect. This initiative requires, in part, as a condition of membership to The DMA, that companies, which market to consumers, participate in The DMA's mail and telephone preference services. These services are offered free of charge to consumers, giving them the ability to remove their names from the lists of national marketers, substantially reducing their mail and telephone marketing calls. More-

over, companies would have to provide notice to consumers if they transfer data to others and provide the consumer the ability to opt-out of such transfers.

Second, shortly, The DMA will launch an e-mail preference service. This service will allow individuals to remove their e-mail addresses from marketing lists in a similar manner to that used in the telephone and mail preference services. This ambitious undertaking is aimed at empowering consumers while also preserving the many societal benefits of marketing continuing to expand in the interactive economy. Once the e-mail preference service is up and running, participation in this service will also be a requirement of DMA membership.

These two efforts will complement the multitude of already existing and ongoing initiatives that compose a robust and effective self-regulatory framework for online privacy. These initiatives include:

- The DMA's award-winning guide for parents, children and educators created in an effort to ensure child safety online
- The Privacy Policy Generator≤A program on our web site which hundreds of companies have used to create privacy policies
- Active support and participation in the P3P privacy technology, which will automatically inform consumers if a web site's privacy practices differ from their privacy preferences, allowing consumers to "negotiate" over those practices
- Development of strong privacy guidelines for marketing online that are enforced by The DMA's Ethics Policy Board with the authority to publicly censure, suspend, or expel members

We believe that the efforts of The DMA and its members continue to prove the utility of effective self-regulation in the online environment. We congratulate the Chairman for his interest and exploration of these issues, and look forward to working with the Courts and Intellectual Property Subcommittee.

STATEMENT

*I. Introduction*

Good morning, Mr. Chairman, and thank you for the opportunity to appear before your subcommittee as it examines online privacy issues. I am Jerry Cerasale, Senior Vice President of Government Affairs for The Direct Marketing Association, Inc. ("The DMA").

The DMA is the largest trade association for businesses interested in direct, database, and interactive marketing and electronic commerce. The DMA represents more than 4,500 companies in the United States and 54 foreign nations. Founded in 1917, its members include direct marketers from 50 different industry segments, as well as the non-profit sector. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses and a host of other segments, as well as the service industries that support them.

The DMA member companies have a major stake in the success of electronic commerce, and are among those most likely to benefit immediately from its growth. The DMA's leadership role is continuing to evolve in the Internet and electronic commerce areas with the Association's recent acquisitions of the Internet Alliance and the Association for Interactive Media. Members of The DMA include Lands' End, L.L. Bean, Time Inc., Dell Computer, Gateway 2000, DoubleClick, autobytel.com, CDW, Micro Warehouse, BMG Direct, Charles Schwab & Co., Lucent Technologies, Bell Atlantic, CheckFree, DLJdirect, eBay, Prodigy Acxiom, AT&T, America Online, IBM, MCI WorldCom, and many others. The DMA has been working diligently to apply its successful self-regulatory system from the traditional media to the Internet and its World Wide Web.

Today I will discuss The DMA's long-time commitment to self-regulation and peer regulation, and our work on a number of public education, technology and self-regulatory initiatives that advance privacy and consumer choice in the online environment. We continue to examine how best to ensure that consumers are afforded opportunities both to learn about products and services of interest to them and to express and obtain their preferences regarding marketers' collection, use, or dissemination of information about them. We are particularly pleased that the Online Privacy Alliance≤of which The DMA is a signatory, BBBOnline, TrustE, and others have joined us in this effort for effective self-regulation on the Internet.

Mr. Chairman, The DMA is convinced that self-regulation and technology are the most effective methods for establishing privacy protection in the borderless world of the Internet, and must be the cornerstone of any domestic or global approach for

ensuring privacy online. As reinforced recently by the Georgetown Internet Privacy Policy Study, self-regulation of privacy on the Internet is working. The Georgetown study indicates that significant progress with respect to Web privacy policies has been made in less than a year since the announcement of the Online Privacy Alliance principles and the release of the FTC study on online privacy. The fact that this progress is already reflected in business practices is particularly encouraging given that a multitude of new self-regulatory programs continue to be developed. Industry self-regulatory principles, consumer choice technologies, and an extensive educational campaign are now in place to create a privacy regime that is both flexible and effective—requirements for the Information Age.

For DMA members, the main use of information collected over the Internet is for marketing purposes. For example, a site may remember that I purchased a particular product there previously and direct me to the same section of its online store. This type of personalization is one of the unique attributes of the Internet that is driving its growth. Any "harm" associated with the collection and use of information in such contexts is minimal, and outweighed by the beneficial uses of the information such as improving the visitor's experience.

Nonetheless, The DMA believes that visitors to Web sites should be informed of a site's information practices and have the opportunity to express and obtain their preferences regarding marketers' collection, use, or dissemination of information about them. When visitors who care to evaluate the site's practices are informed of them, they can make an informed decision about whether to enter the site or take their business elsewhere. The DMA has developed special Online Marketing Principles that embrace these concepts. The DMA also is in the final stages of developing an e-mail preference service that will allow consumers the choice of removing their email addresses from marketing lists used by DMA members. Additionally, The DMA is actively promoting a technology, P3P, that will enable users to receive this information in a convenient, seamless fashion, with enhanced capabilities such as the ability to negotiate with the site over its practices as described below.

I would also like to mention that last fall The DMA supported the passage of the Children's Online Privacy Protection Act. The DMA supported this legislation because we believe that young children present a special case. Unlike adults, children may not fully understand choices regarding privacy. Based in part on existing guidelines developed and followed by The DMA, this legislation contains strong protections for children, prohibiting the collection or distribution of personally identifiable information from children under 13 without prior parental consent or direct parental notification. The DMA is currently working with the Federal Trade Commission as it develops regulations to implement this Act.

*II. Self-Regulation On The Internet Is Resulting In Effective Consumer Privacy And Empowerment As Electronic Commerce Rapidly Continues To Grow*

Since the inception of the commercial Internet, the United States and numerous governments around the world have allowed for the unfettered development of this medium by adopting a "hands-off" approach coupled with industry self-regulation. Without question, this approach is working.

For adults, consumer empowerment tools together with appropriate notice and choice provide the best means for protecting privacy. Self-regulation is better suited for the Internet than legislation as the diversity and technology of this medium foster an environment that is responsive to market forces. This medium is truly global in nature, and the technology is changing rapidly with new issues and solutions thereto emerging daily. Companies at the forefront of the Internet's development truly appreciate how to address consumer concerns without stifling the growth of the medium.

*A. Progress From Industry Self-Regulatory Efforts For Internet Privacy Is Significant*

With the recent explosion of the commercial Internet, The DMA has worked intensively on a number of public education, technology and self-regulatory initiatives that advance privacy and consumer choice in the online environment. Due in large part to the efforts of our members, self-regulation on the Internet is working.

This conclusion is reinforced by the recent results of Georgetown Internet Privacy Policy Study. The study shows that 94 percent of the top 100 web sites have posted a privacy policy notice or an information practice statement. When considered in light of the fact that the experiences of a majority of Internet users are dominated by visits to the more popular sites, it is clear that meaningful and effective privacy practices do currently exist online for consumers. Moreover, there has been a significant increase in the number of policies posted in the past year. In fact, close to 66

percent of all sites now post privacy policies, up from 14 percent in last year's FTC study.

Since January 1998, The DMA has scanned many sites on the Web and directly contacted those sites that did not have a privacy policy posted. The improvement in privacy practices of Web sites reflects the progress made as a direct result of efforts to familiarize industry with appropriate online information practices. To be certain, this is just the beginning. Although the Georgetown study indicates significant progress in the number of privacy polices on web sites, there still exists room for improvement in the content of the privacy policies. The study showed that most of the sites do not yet include all of the elements set out in the Online Privacy Alliance Principles. However, 87 percent of sites provide notice with 77 percent providing choice. These statistics are significant to The DMA as notice and choice empower consumers to determine the uses of their information.

The improvements in both the number of Web sites posting privacy policies and the quality and effectiveness of those policies will continue as more companies and individuals are educated about online information practices. Some of the privacy seal programs that have developed specific and detailed criteria to comply with the Online Privacy Alliance Principles are just recently, after much development, beginning to accept applicants to their programs.

*B. Electronic Commerce Continues To Grow Rapidly*

All evidence continues to indicate that electronic commerce is growing at a unprecedented rate. As the Georgetown study attests, this pace should continue as improvements in privacy practices reinforce consumer confidence in online transactions. The DMA believes that the Congress should be particularly hesitant to enact laws that may disrupt the exponential growth of the Internet, particularly as companies are developing responsible business practices in this medium without regulation.

In addition to the strong indications that self-regulation is working for Internet privacy, the facts continue to make clear that consumers are not reluctant to engage in Internet commerce or to use the Internet. Internet usage continues to increase dramatically, with the number of user computers connected to the Internet having increased in the period from January 1998 to January 1999 from 29 million to more than 43 million. Likewise, revenues from Internet transactions are expected to rise in some estimations to more than $330 billion in 2002 up from $26 billion in 1997. We anticipate that these numbers will continue to grow.

*III. The DMA And Others In Industry Continue To Develop And Implement Self-Regulatory Regimes That Are Providing Effective Protection Of Privacy Online*

As the impact of self-regulation on Internet privacy is being recognized and e-commerce continues to grow, The DMA is continuing to improve its self-regulatory efforts to empower consumers. In the next two months, The DMA will implement two self-regulatory initiatives that will further demonstrate the tenacity of industry in acting responsibly on this issue. First, on July 1, 1999, The DMA Privacy Promise goes into effect. This initiative requires, as a condition of membership to The DMA, that companies participate in The DMA's mail and telephone preference services. These services are offered free of charge to consumers, giving them the ability to remove their names from the lists of national marketers, substantially reducing their mail and telephone marketing calls. Moreover, companies would have to provide notice to consumers if they transfer data to others and provide the consumer with the ability to opt-out of such transfers.

Second, The DMA will soon launch an e-mail preference service. This service will allow individuals to remove their e-mail addresses from marketing lists in a manner similar to that used in the telephone and mail preference services. This ambitious undertaking is aimed at providing consumers choice while continuing to expand in the interactive economy. Once the e-mail preference service is up and running, participation in this service will also be a requirement of DMA membership. This will include the requirements of notice of transfer to others and opt-out of such transfers.

The privacy policies adopted by individual companies are subject to enforcement by the FTC and state attorneys general. By publicly posting policies consistent with criteria set out in the DMA and Online Privacy Alliance guidelines, companies become themselves subject to deceptive practice enforcement actions under existing federal and state consumer protection law if they do not comply with their stated policies. Thus, this self-regulatory framework is far more than a system of voluntary compliance.

These two efforts will complement the multitude of existing and ongoing initiatives of The DMA that compose a robust and effective self-regulatory framework for online privacy. We describe these efforts below.

*A. Online Privacy Principles*

The DMA has been at the forefront of developing effective, responsible self-regulatory codes governing the uses and transfer of information by the direct marketing industry. The cornerstone of the industry's self-regulatory codes is The DMA's *Guidelines for Ethical Business Practice*. These guidelines apply to marketing in all media including the Internet. In addition, The DMA has developed *Privacy Principles and Guidance for Marketing Online* in order to explain and highlight the issues unique to online and Internet marketing.

The DMA, as a result of its extensive membership, has been very effective in establishing industry-wide compliance with its various codes and guidelines. Through its Committee on Ethical Business Practice, a peer review program, The DMA responds to cases of alleged *Guideline* violations brought to its attention by an array of sources—business, consumers, public officials, and the media. This peer-review process is effective. Most cases are resolved through cooperation with the Committee and its recommendations. Members that do not resolve complaints cooperatively are also subject to review by The DMA Ethics Policy Committee with the potential for suspension, expulsion, or censure. The DMA has initiated a process that reveals all cases and their resolution. Furthermore, where the subject company has not agreed to follow guidelines after review, its name is publicly disclosed. In instances where violations of law are also found, the Committee refers matters to the appropriate law enforcement agencies.

*B. Public Education*

The DMA has a vital interest in educating its members and the general public about the responsibilities of people who collect and use data, as well as educating consumers about the process. As a result, The DMA has developed a Web page devoted to privacy and launched its Privacy Action Now and Privacy Promise initiatives.

The DMA has made a special effort to empower children, parents, educators, and librarians by establishing its http://www.cybersavvy.org Web page for them and providing them with tools, information, and resources to ensure safe Web surfing. Additionally, we have produced a "hard copy" version of the Web site, *Get CyberSavvy!*. (available on-line) *Get CyberSavvy* has the distinction of being awarded first place honors for excellence in consumer education by the National Association of Consumer Affairs Administrators.

*C. Technology Solutions*

In light of the unique characteristics of the Internet, technology will play an important role in helping users determine and enforce the ways that information about them is used and collected. The DMA and marketers have been, and continue to be, instrumental in the development of this important technology by encouraging, supporting, indeed helping develop and promote, such software. Under this approach, it will be the individual users, rather than industry or government, who will determine the uses of their personal information.

An initiative that supports this concept, the Platform for Privacy Principles or P3P, will soon be available. This initiative, undertaken by the World Wide Web Consortium, is developing a "negotiation" approach for protecting privacy. A broad coalition of information providers, advertising and marketing specialists, software developers, credit services, telecommunications companies, and consumer and online advocates are working together on P3P to achieve a technological solution that will protect privacy without hindering the development of the Internet as a civic and commercial channel. P3P allows a user to agree to or modify the privacy practices of a web site, and be fully informed of the site's practices before interacting with or disclosing information to a site.

This approach will use "negotiation" or "handshake" technology to cater to an individual's privacy preferences with specificity and effectiveness not available in other media. P3P will allow Webmasters to classify information practices on their sites according to a uniform classification system, and enable consumers to "set" personal privacy preferences within their Web browsers. When a consumer visits a Web site that collects information from visitors, the Web site will collect and use personal information of the consumer only according to the consumer's pre-set preferences.

The DMA also has created and made available from its Web site a technical tool that allows companies to create and post effective privacy policies. This Privacy Policy Generator (http://www.the-dma.org/policy.html) enables companies to develop

customized privacy policies for posting on their web sites based on the companies' policies regarding the collection, use, and sharing of personal information. The utility of this tool, and the ease with which it is used, is demonstrated by the more than 700 companies that have used it and have sent policies to The DMA for review.

*IV. Conclusion*

The DMA believes self-regulation and technology initiatives alike, backed by enforcement of existing laws, offer the most effective means to protecting the privacy of individuals in their interaction with Web sites, while ensuring that consumers are afforded opportunities to learn about products and services of interest to them. This approach is already allowing electronic commerce to flourish, while at the same time enabling the development of a privacy regime that is flexible and effective for the Information Age. We congratulate the Chairman for his interest in and exploration of these issues, and look forward to working with the Courts and Intellectual Property Subcommittee.

Mr. GOODLATTE. Thank you.

Ms. Lesser, welcome.

## STATEMENT OF JILL LESSER, VICE PRESIDENT, DOMESTIC PUBLIC POLICY, AMERICAN ONLINE, INC.

Ms. LESSER. Thank you, Mr. Chairman, members of the subcommittee. I appreciate the opportunity to be here today to discuss online privacy with you on behalf of America Online, a company that knows very well the value of privacy and the importance of the online medium.

The online medium is quickly revolutionizing the way we learn, communicate and do business. It impacts industries as diverse as booksellers and brokers and also consumers with unprecedented opportunities in convenience. Our customers can sign on to AOL and instantaneously do research, send a letter and find the best deal on an airline ticket, tasks that a few short years ago would have consumed far more of their time. But the technology of the Internet offers something even more unique, the ability to customize and personalize their online experiences.

Consumers can communicate specific preferences online that will allow them to receive services or information targeted to their personal needs. For example, an AOL member can set up her online preferences to get the weather forecast for her own ZIP code, read news stories about her professional interest, or get a notice about the availability of a new CD from her favorite musician.

Still, the power of the Internet can only be fully realized if consumers feel confident that their online privacy is protected. For AOL, protecting our consumers' privacy is essential to earning their trust, and trust is crucial to the success of our business. Indeed, AOL learned this important lesson through our own mistake not long ago when an AOL employee was lured into wrongly revealing one of our member's screen names to the government, something we never want to repeat.

Recognizing the importance of building consumer trust, AOL has taken a number of steps to create a privacy-friendly and trust-rich environment. Building on the lessons we have learned and the input we have received from our members, which is critical, we have adopted a privacy policy to clearly explain to our users what information we collect, why we collect it and how members can exercise choice about the use of that information. We have based our policy on core principles that reflect consumer needs and expectation. For example, we will not read a member's private e-mail. We

will not disclose any information to anyone about where a member goes online, and we will not give out a member's phone number, credit card information or screen name without consent.

We give consumers clear choices about how their personal information is used and make sure that our members are well informed about what those choices are. For example, if a customer decides he does not want to receive any marketing materials from us that are targeted to him based on his personal information or preferences, he can simply check a box on our service to let us know, a box that is easy to find and always available.

We also make sure that our policies are well understood and implemented by our employees. We provide training about our privacy policy and require all to sign and agree to abide by a privacy policy as a condition of employment, and we continually review state-of-the-art technology to ensure the most advanced technologies possible to defend consumer data security.

We take extra steps to protect the safety of children online and have created a special environment called Kids Only that allows people to make sure that their children do not interface with strangers or allow strangers to contact their children, and our parental controls allow parents to set safeguards so that members make sure that children don't talk to people they really shouldn't.

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners, and we believe this is critical. One of the strongest examples is our certified merchant program, which guarantees our members are satisfied with the merchants they buy from the online environment who participate in this program. We offer a money-back guarantee to dispel consumer concerns about shopping security and increase consumer trust in this powerful medium.

We believe the more work we are able to do with our business partners and require high standards of them, the more likely it is that these standards will become the marketplace norm. As you heard from Christine Varney, we are key supporters of the Online Privacy Alliance and believe that the Georgetown study recently released indicates a lot of progress, more progress than even we would have expected, on an industrywide basis, an industry that is growing so quickly, but as she indicated, our work has only just begun.

We believe the technology is key to this, and we will continue with you, Chairman Goodlatte, to advocate widespread availability of the use of strong encryption to make sure that privacy can be protected across this country and abroad.

And finally, I know I am out of time. Let me just say that we are trying to craft the rules of the road and that good business practices ultimately will dictate whether the industry grows, whether the medium grows and whether e-commerce grows. The challenges that lie ahead will give us the chance to prove we can work together to promote effective online privacy through industry-led, market-driven initiatives with strong government enforcement of laws that prohibit fraud and make certain bad actors on the Net disappear.

Ultimately it is the consumer who will be the judge of whether these efforts are adequate. No matter how extraordinary the oppor-

tunities for electronic commerce may be, we know our business will fail if we cannot meet consumer demands for privacy protection and gain their trust.

I appreciate the opportunity to be here, and I am happy to answer any questions you may have.

Mr. GOODLATTE. [Presiding.] Thank you, Ms. Lesser.

[The prepared statement of Ms. Lesser follows:]

PREPARED STATEMENT OF JILL LESSER, VICE PRESIDENT, DOMESTIC PUBLIC POLICY, AMERICAN ONLINE, INC.

Chairman Coble, Congressman Berman, and Members of the Subcommittee, I would like to thank you, on behalf of America Online, for the opportunity to discuss online privacy with you today. My name is Jill Lesser, and I am the Vice President for Domestic Policy at AOL.

The online medium is quickly revolutionizing the way we learn, communicate, and do business. People are migrating to the Internet to meet their commerce and communications needs at an extraordinary rate because it is convenient and fast, and offers an ever-growing selection of information, goods and services. AOL subscribers can sign on to our service and do research, shop for clothes, and buy airline tickets all in a matter of minutes.

In addition, the online environment offers users unique benefits of customization and personalization. Consumers can communicate specific preferences online that will allow them to receive information targeted to their own interests. For instance, AOL members can set their online preferences to get the weather forecast for their own zip code, read news stories about their own hometown, or receive notices about special discounts on their favorite CDs. No other commercial or educational medium has ever afforded such tremendous potential for personalization.

But the power of the Internet can only be fully realized if consumers feel confident that their privacy is properly protected when they take advantage of these benefits. We know very well that if consumers do not feel secure online, they will not engage in online commerce or communication—and without this confidence, our business cannot grow. For AOL, therefore, protecting our members' privacy is essential to earning their trust, and this trust is in turn essential to building the online medium. We learned this important lesson through our own mistakes not too long ago, when an AOL employee wrongly revealed the screen name of one of our members to the government.

Recognizing the importance of this issue, AOL has taken a number of steps to create an environment where our members can be certain that their personal information and their choices regarding the use of that information are being respected: from creating and implementing our own privacy policies and educating our members about them, to promoting best practices among our business partners, to engaging in industry-wide initiatives and enforcement mechanisms that will raise the bar for all companies who do business online.

Although the Internet is growing at a tremendous pace, we are still only at the beginning of the development of this new medium. Industry initiatives are helping to craft the "rules of the road" that will dictate online business practices, and we believe that it is important to see how those rules develop rather than imposing a sweeping regulatory framework on the Internet and e-commerce. Therefore, we hope to continue working with policymakers, consumer groups, and industry colleagues to promote industry-led, market-driven initiatives that will build on the progress we have already made and ensure that individual privacy is protected online.

*Setting an Example*

AOL is committed to protecting consumer privacy. Building on the lessons we have learned and the input we have received from our members, we have created privacy policies that clearly explain to our users what information we collect, why we collect it, and how they can exercise choice about the use and disclosure of that information. We update our policies and procedures to respond to changes in technology or consumer demand, but our commitment to core privacy protections remains constant. AOL's current privacy policy is organized around 8 core principles:

(1) We do not read your private online communications

(2) We do not use any information about where you personally go on AOL or the Web, and we do not give it out to others.

(3) We do not give out your telephone number, credit card information or screen names, unless you authorize us to do so. And we give you the opportunity to correct your personal contact and billing information at any time.

(4) We may use information about the kinds of products you buy from AOL to make other marketing offers to you, unless you tell us not to. We do not give out this purchase data to others.

(5) We give you choices about how AOL uses your personal information.

(6) We take extra steps to protect the safety and privacy of children.

(7) We use secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information.

(8) We will keep you informed, clearly and prominently, about what we do with your personal information, and we will advise you if we change our policy.

We give consumers clear choices about how their personal information is used, and we make sure that our users are well informed about what those choices are. For instance, if an AOL subscriber decides that he does not want to receive any targeted marketing notices from us based on his personal information or preferences, he can simply check a box on our service that will let us know not to use his data for this purpose. Because we know this issue is so critically important to our members and users, we make every effort to ensure that our privacy policies are clearly communicated to our customers from the start of their online experience, and we notify our members whenever our policies are changed in any way.

We also make sure that our policies are well understood and properly implemented by our employees. We require all employees to sign and agree to abide by our privacy policy, and we provide our managers with training in how to ensure privacy compliance. We are committed to using state-of-the-art technology to ensure that the choices individuals make about their data online are honored.

Finally, we try to keep users informed about the steps they can take to protect their own privacy online. For instance, we emphasize to our members that they must be careful not to give out their personal information unless they specifically know the entity or person with whom they are dealing, and we encourage them to check to see whether the sites they visit on the Web have posted privacy policies.

*Protecting Children Online*

AOL takes extra steps to protect the safety and privacy of children online. One of our highest priorities has always been to ensure that the children who use our service can enjoy a safe and rewarding online experience, and we believe that privacy is a critical element of children's online safety.

We have created a special environment just for children—our "Kids Only" area—where extra protections are in place to ensure that our children are in the safest possible environment. In order to safeguard kids' privacy, AOL does not collect personal information from children without their parents' knowledge and consent, and we carefully monitor all of the Kids Only chat rooms and message boards to make sure that a child does not post personal information that could allow a stranger to contact the child offline. Furthermore, through AOL's "Parental Controls," parents are able to protect their children's privacy by setting strict limits on whom their children may send e-mail to and receive e-mail from online.

Because of the unique concerns relating to child safety in the online environment, AOL supported legislation in the 105th Congress to set baseline standards for protecting kids' privacy online. We worked with Senator Bryan, the FTC, and key industry and public interest groups to help bring the Child Online Privacy Protection Act (COPPA) to fruition last year. We believe the enactment of this bill was a major step in the ongoing effort to make the Internet safe for children.

*Fostering Best Practices*

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners and industry colleagues. One of the strongest examples of this effort is our "Certified Merchant" program, through which we work with our business partners to guarantee our members the highest standards of privacy and customer satisfaction when they are within the AOL environment. AOL carefully selects the merchants we allow in the program (currently there are over 150 participants), and requires all participants to adhere to strict consumer protection standards and privacy policies. The Certified Merchant principles are posted clearly in all of our online shopping areas, thereby ensuring that both consumers and merchants have notice of the rules involved and the details of the enforcement mechanisms, which help to foster consumer trust and merchant responsiveness.

Here are the criteria that our merchants have to meet in order to become certified and to display the America Online Seal of Approval (some screen shots that show how these criteria appear to subscribers on our service are attached to this testimony):

1. Post complete details of their Customer Service policies, including: Contact Information, Shipping Information, Returns Policies, and Money-Back Satisfaction Guarantee Information.
2. Receive and respond to e-mails within one business day of receipt.
3. Monitor online store to minimize/eliminate out-of-stock merchandise available.
4. Receive orders electronically to process orders within one business day of receipt.
5. Provide the customer with an order confirmation within one business day of receipt.
6. Deliver all merchandise in professional packaging. All packages should arrive undamaged, well-packed, and neat, barring any shipping disasters.
7. Ship the displayed product at the price displayed without substituting.
8. Agree to adopt privacy policies that comport with AOL's privacy policy.

Through our Certified Merchant program, we commit to our members that they will be satisfied with their online experience, and we have developed a money-back guarantee program to dispel consumer concerns about shopping online and increase consumer trust in this powerful new medium. We believe that these high standards for consumer protection and fair information practices will help bolster consumer confidence and encourage our members to engage in electronic commerce.

*Helping to Promote Industry Efforts*

The online industry as a whole is taking positive steps toward protecting consumer privacy. In fact, to improve industry's commitment to online privacy, AOL joined with other companies and associations last year to form the Online Privacy Alliance (OPA), a group dedicated to promoting privacy online.

The OPA has worked hard to develop a set of core privacy principles—centered around the key concepts of notice, choice, data security, and access—and its members are committed to posting and implementing privacy policies that embody these principles. Since we began our efforts just a few months ago, the OPA has grown to include more than 85 recognized industry leaders, and industry efforts to protect consumer privacy online have blossomed.

A recent study conducted by Georgetown University Professor Mary Culnan shows that, in a sample drawn from a pool of the 7500 most visited websites, more than 65% of the sites have posted a privacy policy or a statement about their information practices. This number demonstrates a tremendous increase from the number of sites posting policies just one year ago, when the FTC conducted a similar study. We believe that private sector leadership in developing fair information practices is the right approach to assuring broad privacy protection online, but we also realize that there is still more work to be done. In order to build on our preliminary success, the OPA has renewed its commitment to reach out to businesses nationwide to explain the importance of protecting online privacy and posting meaningful privacy policies.

We believe that the OPA member companies are setting a new standard for online privacy, and that as consumers become more aware of the choices available to them, the marketplace will begin to demand robust privacy polices of all companies that do business online. But we also understand the need for meaningful enforcement of industry standards. That's why we abide by the OPA requirement to participate in robust enforcement mechanisms through our involvement in the TrustE and BBBOnline privacy seal programs. We are key sponsors of both the TrustE and BBBOnline privacy seal programs, and have worked closely with industry representatives and members of the academic community to help formulate strict standards for seal eligibility.

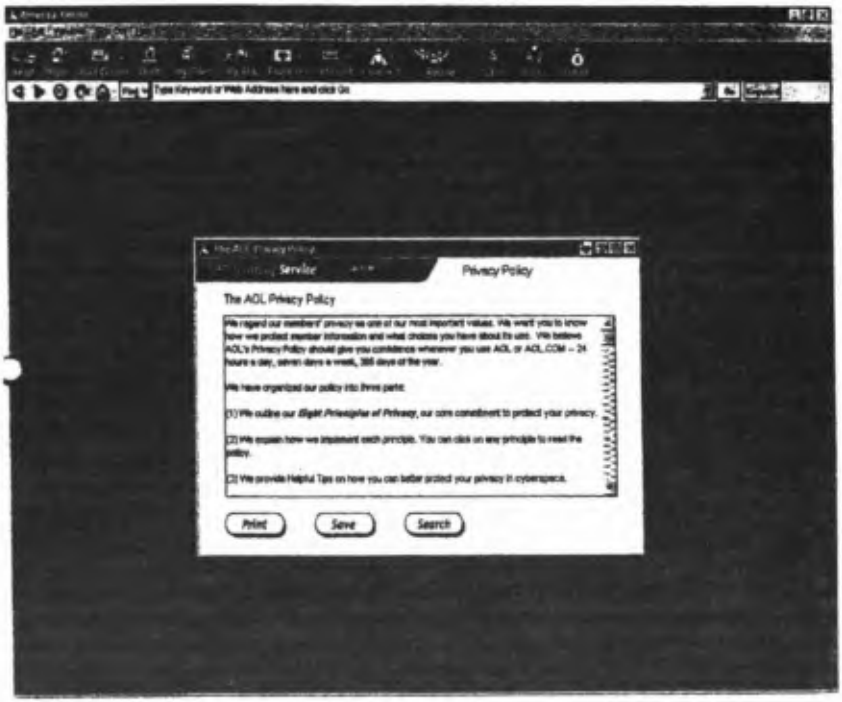
*The Challenges Ahead*

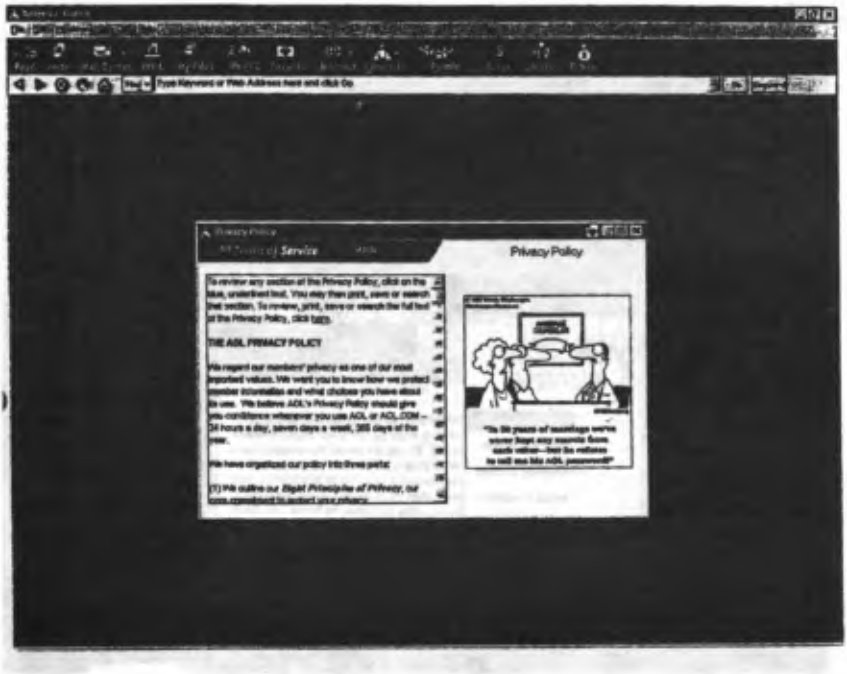
It is clear that companies are responding to the increasing marketplace demand for online privacy, and that the tremendous growth of e-commerce reflects positive trends on a variety of consumer protection issues, including privacy. But our work has only just begun. As technology makes it easier for companies to collect and use personal information, the adoption and implementation of robust privacy policies will become even more important.

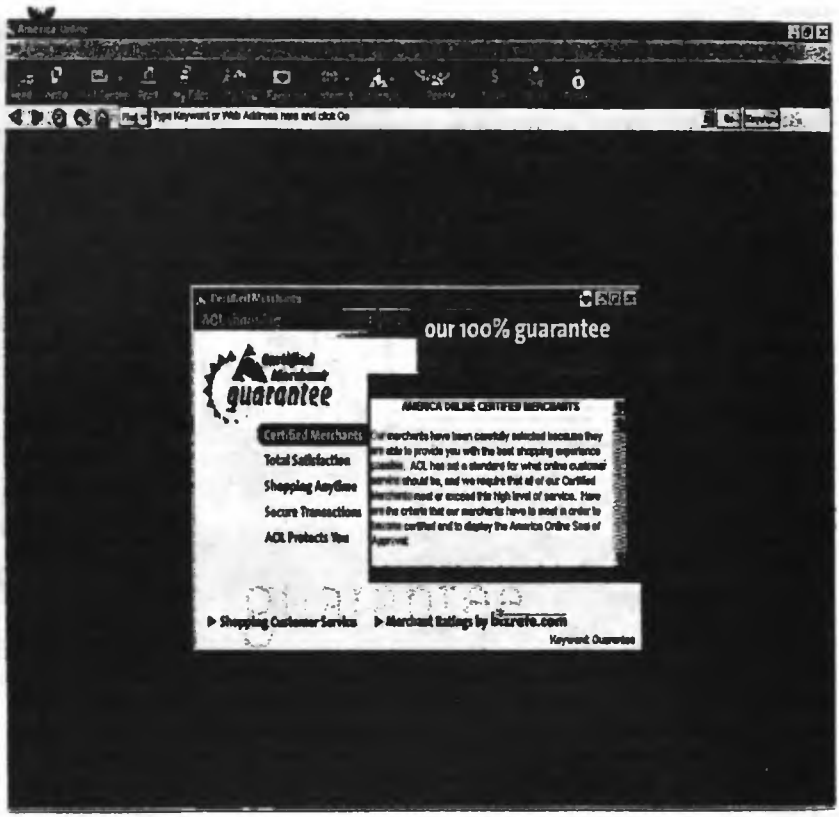
In part, we believe that technology holds the key to ensuring a safe and secure online environment. As an online service provider, we believe it is critical for us to be able to provide the most sophisticated security technologies to our members so that they can take steps to protect their own privacy online. That's why we will continue to advocate the widespread availability and use of strong encryption, both in this country and abroad.

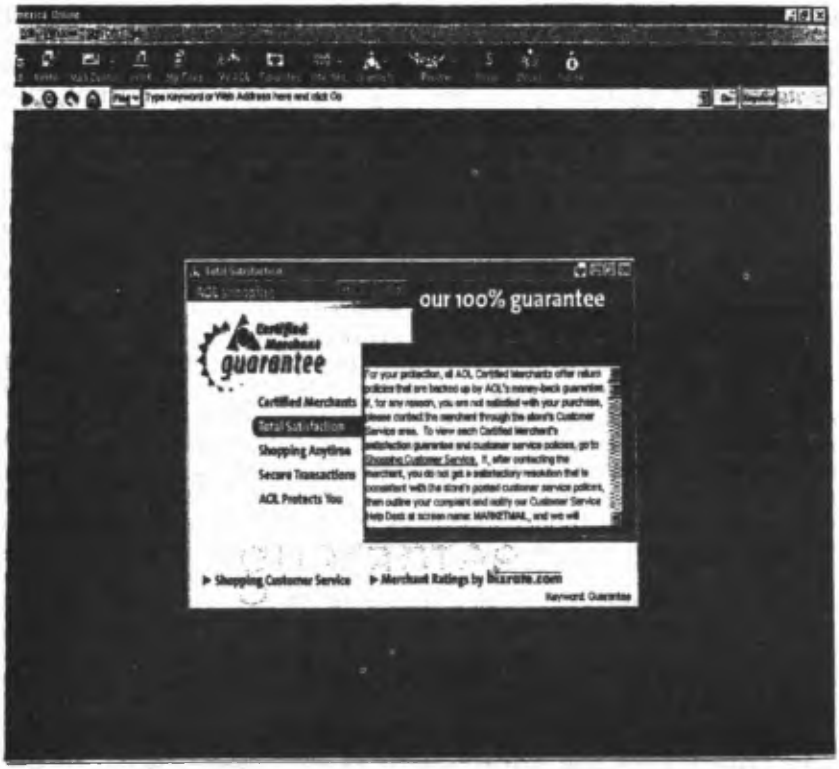
The challenges that lie ahead will give us the chance to prove that industry and government can work together to promote online privacy. But ultimately, it is the consumer who will be the judge of whether these efforts are adequate. Because no matter how extraordinary the opportunities for electronic commerce may be, the marketplace will fail if we cannot meet consumers' demands for privacy protection and gain their trust.

We at AOL are committed to doing our part to protecting personal privacy online. Our customers demand it, and our business requires it—but most importantly, the growth and success of the online medium depend on it. We appreciate the opportunity to discuss these important issues before the Committee, and look forward to continuing to work with you on other matters relating to the Internet and electronic commerce.




Service
Privacy Policy
THE AOL PRIVACY POLICY


our 100% guarantee
guarantee
Certified Merchants
Total Satisfaction
Shopping Anytime
Secure Transactions
AOL Protects You
AMERICA ONLINE CERTIFIED MERCHANTS
Shopping Customer Service
Merchant Ratings by bizrate.com




Mr. GOODLATTE. I want to thank the real chairman of this committee, Mr. Coble, for allowing me to sit here and continue to conduct this hearing.

Mr. Rotenberg.

## STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Congressman, Mr. Chairman, members of the subcommittee.

I wish I could join the chorus this morning in support of industry self-regulation and say that the privacy problems on the Internet have largely been resolved, but the reality tells a different story because the United States in 1999 sees now a national protest against new products and services that threaten individual privacy. We have seen campaigns against Intel for their computer chip, against Microsoft for a universal identifier, and more than a quarter of a million Americans commented on an obscure banking regulation because of their concerns about the protection of their personal information.

This morning the New York Times reports that negotiations between the United States and Europe are breaking down over the central question of transborder data flows and whether the United States has adequate privacy protection to protect the interests of European citizens.

So my view of where we are today is perhaps not quite so bright as those who are seated with me at this table. I do think that in our traditions there are ways to develop privacy safeguards in law that can be enforced that provide simple, predictable uniform rules that are good for businesses and good for customers. I think that is the approach that we should be taking online.

The problems with the Georgetown survey are many, and my testimony goes into them in some detail, but the primary problem is that the survey shows in the 2 years since my organization, EPIC, conducted the first comprehensive survey of Internet privacy policy, that we have constantly lowered the bar about what constitutes a privacy policy to try to show progress, so much so that when it is reported today that 66 percent of Web sites have a privacy policy, let me tell you what that policy constitutes.

It could be a statement that simply says, "we collect personal information about you." That is a privacy policy under the Georgetown survey. It goes into the 66 percent box. "We disclose personal information to others." That is also a privacy policy. "We use 40-bit crypto for network communications." That is a privacy policy, and if you add the statement "we are not responsible for errors, and if you have questions, send us e-mail," you have hit all five buttons. You get a gold star for having a comprehensive privacy policy.

That is a nonprivacy policy and reflects the growing effort to lower the standard for what constitutes privacy protection in this country. But there are some other real consequences as well that I think would be of particular interest to you and to the other members of the subcommittee.

We are seeing at EPIC in our comparison between countries that have privacy laws and privacy agencies and those that do not that the countries with comprehensive legal frameworks are doing a better job of developing new technologies and resolving new technology challenges that have privacy implications. For example, in the area of encryption we see that countries that have privacy agencies uniformly support the availability of strong encryption techniques and want to see those techniques made widely available. Where privacy agencies don't exist, export controls limit the availability of encryption and other privacy techniques.

Other issues, cookies, for example, which raise complicated privacy problems on the one hand, no one doubts that there are benefits for cookies for online shopping and commerce on the Internet, but there are also privacy issues. How do you resolve these in a way to maximize the opportunity that the technology provides while minimizing the privacy risk?

Again, those countries with comprehensive legal frameworks and privacy agencies are doing a better job looking out for the interests of users on the Internet than those countries that are not taking this approach.

Now, I know it is very difficult today to argue for legislation or even the creation of a new Federal agency, and certainly people would like to see self-regulation work. My organization, EPIC, has opposed many efforts to regulate the Internet, and we recognize the tremendous opportunity that it provides, but at the end of the day, the question is not whether self-regulation works. The question is

whether privacy protection works, and our view is that today self-regulation is not making privacy protection work.

So thank you very much. I will be pleased to answer your questions.

Mr. GOODLATTE. Thank you, Mr. Rotenberg.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

My name is a Marc Rotenberg. I am the Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, DC.[1] I appreciate the opportunity to testify today before the Subcommittee of Courts and Intellectual Property regarding Electronic Communications Privacy Policy Disclosures.

The protection of privacy is quickly emerging as a central concern for Americans as we approach the twenty-first century. In the past year we have seen national protests launched against companies that design computer chips and computer software that could endanger personal privacy. More than a quarter of a million Americans opposed a banking regulation that would have established extensive government reporting requirements on routine financial transactions. And polls routinely show that the lack of privacy protection is contributing to growing public unease about the use of the Internet for commercial transactions. Will privacy policies actually protect the privacy rights of Americans in the years ahead?

Simply stated, I believe that the current efforts to promote industry self-regulation will not adequately address the public concerns about privacy and the Internet. Industry policies are typically incomplete, incoherent, and unenforceable. They are having little impact on actual data collection practices. Instead of reducing the demand for personal information or encouraging the development of privacy enhancing techniques, industry privacy policies are literally papering over the growing problem of privacy protection online.

A better approach would be to establish a legal framework that provides simple, predictable, uniform rules to regulate the collection and use of personal information. Not only is this approach consistent with US privacy legislation, it would also provide clarity and promote trust for consumers and businesses in the new online environment. I also believe that protecting privacy rights in law would encourage the development of better techniques to protect privacy and, in the long term, reduce the need for government intervention. The key is to pursue the enforcement of Fair Information Practices and the development of methods that reduce the need for personally identifiable information.

PRIVACY PROTECTION AND THE ROLE OF FAIR INFORMATION PRACTICES

Up until a few years ago, legislating privacy protection was a straightforward problem. The basic goal was to outline the responsibilities of organizations that collect personal information and the rights of individuals that give up personal information. These rights and responsibilities are called Fair Information Practices and they help ensure that personal information is not used in ways that are inconsistent with the purpose for which they were collected. Fair Information Practices typically include the right to limit the collection and use of personal data, the right to inspect and correct information, a means of enforcement, and some redress for individuals whose information is subject to misuse.[2]

Fair Information Practices are in operation in laws that regulate many sectors of the US economy, from companies that grant credit to those that provide cable television services.[3] Your video rental store is subject to Fair Information Practices as are public libraries in most states in the country. The federal government is subject to the most sweeping set of Fair Information Practices. It is called the Privacy Act of 1974 and it gives citizens basic rights in the collection and use of information

[1] The Electronic Privacy Information Center is a project of the Fund for Constitutional Government, a non-profit charitable organization established in 1974 to protect civil liberties and constitutional rights. More information about EPIC is available at the EPIC web site http://www.epic.org.

[2] See generally, Robert Gellman, "Does Privacy Law Work?" in P. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press 1998)

[3] M. Rotenberg, *The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments* 1–37, 95–97 (Fair Credit Reporting Act of 1970, Cable Communications Policy Act of 1984) (EPIC 1998) [hereinafter *Privacy Law Sourcebook*]

held by federal agencies. It also imposes on these same agencies certain obligations not to misuse or improperly disclose personal data.[4]

The current debates in Congress over protecting medical records and financial records follow in this tradition. And privacy laws in these areas will reflect the rights that Congress is prepared to extend to patients and bank customers who seek to safeguard their personal information.

Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection. The most well known of these international guidelines are the OECD Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[5] The OECD Privacy Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation.[6] These are:

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

It is worth noting also in the United States that there is a particularly strong tradition of extending privacy rights to new forms of technology. So for example, subscriber privacy provisions were included in the Cable Act of 1984. New protections for electronic mail were adopted in the Electronic Communications Privacy Act of 1986.[7] Video rental records were safeguarded as a result of the Video Privacy Protection Act of 1988.[8] And auto-dialers and junk faxes were regulated by the Telephone Consumer Protection Act of 1991.[9]

Viewed against this background, the problem of privacy protection in the United States in the early 1990s was fairly well understood. The coverage of US law was

---

[4] *Privacy Law Sourcebook* 38–54.

[5] *The Privacy Law Sourcebook* 161–87.

[6] BASIC PRINCIPLES OF NATIONAL APPLICATION

*Collection Limitation Principle.* There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

*Data Quality Principle.* Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

*Purpose Specification Principle* The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

*Use Limitation Principle.* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

*Security Safeguards Principle.* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

*Openness Principle* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

*Individual Participation Principle.* An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

*Accountability Principle.* A data controller should be accountable for complying with measures which give effect to the principles stated above.

*Privacy Law Sourcebook* 163–64.

[7] *Privacy Law Sourcebook* 98–131.

[8] *Privacy Law Sourcebook* 132–34.

[9] *Privacy Law Sourcebook* 144–52.

uneven: Fair Information Practices were in force in some sectors and not others. There was inadequate enforcement and oversight. Technology continued to outpace the law. And the Europeans were moving forward with a comprehensive framework to safeguard privacy rights of their citizens.

Unfortunately, just at the point in time when there was need for leadership in government to promote a privacy policy based on extending Fair Information Practices, the administration and Congress turned away from well established legal standards and traditions and proposed instead a search for solutions based on industry self-regulation.

Some said that the interactive nature of the Internet made possible a new approach to privacy protection, one that focused on individuals exercising privacy "choice" or "preferences." But providing a range of choices for privacy policies turns out to be a very complicated process, and there is no guarantee that a person's privacy preferences on one day will be the same the next. In the rush to avoid a "one size fits all approach," those who focused on privacy choices may have discovered paradoxically that "many sizes fits none." In other words simple, predictable, uniform rules make it easier for individuals to exercise control over their personal information, than an endless selection of choices that turn out to be meaningless.

Other industry approaches emphasized the easy online availability of privacy policies. But in practice, making use of a web site privacy policy turns out to be cumbersome and impractical, and almost the antithesis of the Internet's architecture. The very networked nature of the Internet that enables users to move freely from one site to the next discourages standards that vary from one site to the next. If a user will click past a site because a graphic takes too long to load, can we reasonably expect that some person to read through the fine print of a privacy policy? Both of these approaches, which are the outcome of pursuing the industry policy of self-regulation, have made it more difficult—not easier—for individuals to protect their privacy online.

An additional problem was created by the somewhat awkward role of the Federal Trade Commission. Because the United States lacks an agency with the expertise and competence to develop privacy policies, the FTC was cast in the role of de facto privacy agency. But the FTC did not itself have the authority to enforce Fair Information Practices or to promote the development of the various privacy enhancing techniques that were being pursued by other privacy agencies around the world.[10] The FTC relied instead on its Section 5 authority to investigate and prosecute fraudulent or deceptive trade practices.

The better approach would have been to look at the Internet and ask how could it make it easier to apply and enforce Fair Information Practices. For example, one of the hard problems in privacy protection is ensuring that individuals are able to access and correct information about themselves. In the paper world, the right of access is an elaborate and costly process for both businesses and consumers. Records must be copied and sent by mail. In the online world it is much easier to provide ready access to profile information. In fact many web sites today, from airline reservations to online banking, are making information that they have about their customers more readily available to their customers over the Internet. It is not "choice" that customers are exercising but rather "control" over their personal information held by others.

The Internet is also offering interesting developments in the use of techniques for anonymity and pseudo-anonymity to protect online privacy. These techniques enable commercial transactions while minimizing or eliminating the collection of personal information. Such techniques avoid the need for privacy rules simply by avoiding the rights and responsibilities that result from the collection and use of personal data.

## THE ROLE OF PRIVACY SURVEYS

For the last several years a great effort has been underway to encourage industry groups to develop policies for self-regulation. Self-regulation has been offered as an effective and appropriate way to encourage industry groups to respond to public concerns about privacy without the actual burden of changing practices or reducing the growing dependence on personal information. The critical question that is typically ignored in the quest for solutions based on self-regulation is whether it is an effective means to protect personal privacy.

---

[10] See, e.g., EC Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, "Anonymity on the Internet" (1997) reprinted in *Privacy Law Sourcebook* 331–342.

To understand the problem of privacy protection on the Internet in more detail, in 1997 EPIC undertook the first comprehensive survey of web site privacy practices. We reviewed 100 of the most frequently visited web sites on the Internet.[11] We checked whether sites collected personal information, had established privacy policies, made use of cookies, and allowed people to visit without disclosing their actual identity.

We found that about half of the sites that we surveyed in 1997 collected personal information. This was typically done for on-line registrations, surveys, user profiles, and order fulfillment. We also found that few web sites had explicit privacy policies (only 17 of our sample) and none of the top 100 web sites met basic standards for privacy protection. We also noted that users were unable to exercise any meaningful control over the use of cookies. However, we noted that anonymity played an important role in online privacy, with many sites allowing users to access web services without disclosing personal data. We said that:

> Users of web-based services and operators of web-based services have a common interest in promoting good privacy practices. Strong privacy standards provide assurance that personal information will not be misused, and should encourage the development of on-line commerce. We also believe it is matter of basic fairness to inform web users when personal information is being collected and how it will be used.

We recommended that:

- Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the home page by looking for the word "privacy."
- Privacy policies should state clearly how and when personal information is collected.
- Web sites should make it possible for individuals to get access to their own data
- Cookies transactions should be more transparent
- Web sites should continue to support anonymous access for Internet users.

In 1998 the FTC conducted its own survey of privacy policies. Although the survey looked at more web sites, the FTC survey was in some critical respects narrower than the original EPIC survey.[12] The FTC focused on the number of web sites that collect personal information and also on the number of web sites that had a privacy policy. But the FTC largely ignored the crucial role of anonymity in privacy protection. The FTC also lowered the bar by defining Fair Information Practices to be simply "notice," "choice," "access" and "security."[13] Although we did not look at the full range of Fair Information Practices in 1997, we followed the OECD practice in inquiring whether there were "use limitations" or "secondary use restrictions" in the privacy policies we found. This point is important because much of privacy law turns on the principle of finality—the principle that information is collected for a particular purpose and that information should be used only for that purpose unless meaningful consent is obtained from the data subject.

Not surprisingly, the 1998 FTC survey found an increase in the number of web sites posting privacy policies.

In 1998 we undertook a second survey to determine whether industry was doing a good job encouraging its own members to adopt privacy policies. "Surfer Beware II: Notice is Not Enough" surveyed the privacy policies of 76 new members of the Direct Marketing Association (DMA).[14] We chose the DMA because it has been a leading proponent of self-regulation and because it has undertaken a number of efforts to encourage privacy protection through self-regulation. These included a policy announced in October 1997 that the DMA would require future members to post a privacy policy and provide an opt-out capability. Of the 76 new members we examined, only 40 had Web sites and of these, only eight sites had any form of privacy policy. We examined these policies and found that only three of the new members have privacy policies that satisfied the DMA's requirements set out in October 1997.

---

[11] EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [http://www.epic.org/reports/surfer-beware.html]

[12] FTC, "Online Privacy: A Report to Congress" (1998) [http://www.ftc.gov/reports/privacy3/index.htm].

[13] Prepared statement of the Federal Trade Commission on "Internet Privacy" before the Subcommittee on Courts and Intellectual Property of the House Judiciary Committee, March 26, 1998 [http://www.ftc.gov/os/1998/9803/privacy.htm

[14] [http://www.epic.org/reports/surfer-beware2.html]

None of the sites examined allowed individuals to gain access to their own information. We concluded that the DMA's efforts to promote privacy practices is having little impact on its new members, even after repeated assurances from the DMA that this approach is effective.

Two recent surveys, funded by industry groups, found an increased number of web sites are now posting privacy policies. While many were quick to take this finding as an indication that self-regulation is working, a quick look behind the numbers reveals a different story.[15] Less than 10% of the web sites have privacy policies that include the minimal elements proposed by the FTC. The collection and use of information among commercial web sites is rapidly accelerating.

Taking a step back, I think the survey reveals an even larger problem with the assessment of self-regulation in 1999. It is not simply that there are still a small number of web sites with even the elements of a basic privacy policy, the survey also reflects the continuing process of lowering the bar to establish the success of self-regulation. The most recent survey allows that the posting of just one element of Fair Information Practices could constitute a privacy policy. Thus the industry was able to say, "Of the 364 websites surveyed, 65.7% had posted at least one type of privacy disclosure." At a certain point, you cannot lower the bar any further. I imagine you should simply push it to the side and hope no one accidentally trips over it.

The survey methodology also reflects a lack of interest in the various techniques that would enable privacy protection through anonymity. The German government for example, more than two years ago adopted legislation to encourage the use of anonymity for commercial sites on the Internet. A survey that attempted to measure online privacy in 1999, as compared with our survey in 1997, should move the inquiry forward by trying to determine what techniques were being adopted to protect online privacy and specifically ask about the availability of techniques that would enable users to protect the disclosure of their personal information, particularly in the absence of enforceable Fair Information Practices.

## THE GLOBAL PICTURE

To understand the larger picture of privacy protection, it is necessary to look beyond the United States and the narrow issue of whether web sites post privacy policies. In 1998 EPIC undertook the first comprehensive survey on international privacy laws and practices. The report "Privacy and Human Rights 1998: An International Survey of Privacy laws and Developments" looked in detail at the state of privacy in fifty countries around the world.[16] We found that:

- Privacy is a fundamental human right recognized in all major international treaties and agreements on human rights. Nearly every country in the world recognizes privacy as a fundamental human right in their constitution, either explicitly or implicitly. Most recently drafted constitutions include specific rights to access and control one's personal information.
- New technologies are increasingly eroding privacy rights. These include video surveillance cameras, identity cards and genetic databases.
- There is a growing trend towards the enactment of comprehensive privacy and data protection acts around the world. Currently over 40 countries and jurisdictions have or are in the process of enacting such laws. Countries are adopting these laws in many cases to address past governmental abuses (such as in former East Bloc countries), to promote electronic commerce, or to ensure compatibility with international standards developed by the European Union, the Council of Europe, and the Organization for Economic Cooperation and Development.
- Surveillance authority is regularly abused, even in many of the most democratic countries. The main targets are political opposition, journalists, and human rights activists. The U.S. government is leading efforts to further relax legal and technical barriers to electronic surveillance. The Internet is coming under increased surveillance.

We are currently updating our 1998 survey. Our preliminary results show that more countries are moving to adopt comprehensive privacy legislation. For example, Canada is expected to enact comprehensive federal privacy legislation by the end of June, and many countries in Eastern Europe and East Asia are moving in a simi-

---

[15] "Online Privacy Alliance Says Web Sweeps Confirm Significant Progress in Privacy Self-Regulation," Online Privacy Alliance [http://www.privacyalliance.org/news/05121999.shtml].

[16] EPIC and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice* (EPIC 1998)

lar direction. There are a number of explanations for this, including the desire of countries to trade with the European Union as well as to respond to popular concerns about privacy protection. But there is also the natural tendency in privacy policy toward "convergence" the development of common standards that promote the free flow of information by ensuring the protection of privacy.[17]

OBSERVATIONS

A review of the surveys undertaken over the last several years leads to the following general observations:

First, while it can be shown that more web site operators are posting privacy policies, there is little evidence that this is translating into better privacy protection for Internet users. There is still no effective means of enforcement. No real effort has been undertaken to begin auditing or conduct oversight to ensure that the privacy policies posted are being followed.

Second, just as the number of web site privacy policies has increased, so too have the demands for personal information. Indeed, it would not be too difficult to show that that the collection and use of personal data online over the last few years has far exceeded the development and enforcement of privacy policies. In this respect, the "privacy gap" has widened not narrowed since 1997.

Third, the definition of what constitutes a privacy policy continues to be lowered as time passes. To say that 2/3 of web sites today post a privacy policy and that this shows progress is a bit like saying 2/3 of the cars in a scrapyard have at least one working component. The reality is that only a small percentage of web sites even begin to approach the type of privacy protection that would be provided by the most rudimentary privacy law in this country.

Fourth, there has been a movement away from the consideration of techniques that could protect privacy and reduce the need for legislation. When EPIC undertook the first survey of Internet policies, we were very much aware that anonymity would play a critical role in protecting online privacy. We continue to believe that a much greater emphasis must be placed on developing techniques that reduce the demand for personally identifiable information.

ROLE OF THE FEDERAL TRADE COMMISSION

Much has been made in the last few years about the role of the Federal Trade Commission in defending the privacy rights of Internet users. The FTC has been held out as the de facto privacy agency in the United States and the backstop to enforce Industry self-regulatory policies. And while it is clearly the case that the FTC has expressed great interest in privacy issues, almost four years after it was asked by Congress to investigate the privacy risks associated with computerized databases, the FTC has produced little in the way of privacy assistance or enforcement for Internet users.[18]

In the past three years, the FTC has rendered an opinion in a privacy case about once a year. Which is to say the enforcement of privacy rules comes as often at the FTC as does Christmas. By comparison, the Information and Privacy Commissioner of the Canadian province of British Columbia has issued 200 orders in the same time period.[19]

Interestingly, one of the ongoing problems with the FTC's investigation of privacy complaints is the lack of transparency into the agency's own practices for pursuing privacy investigations. Earlier this year, there was a national campaign to stop the release of a computer chip that would enable ubiquitous identification across the Internet. While this technique may have provided some benefits in certain commercial applications, there was little doubt it would also raise enormous privacy issues.

EPIC, Privacy International, and Junkbusters, the groups that organized the campaign against the Intel chip wrote to the FTC to see if the FTC has the authority to investigate what many would agree is one of the biggest privacy issues so far in

[17] Colin Bennett, *Regulating Privacy* (Cornell 1992).

[18] Letter from EPIC Director Marc Rotenberg to FTC Commissioner Christine Varney (December 14, 1995) ("I am writing to you to urge the Federal Trade Commission to investigate the misuse of personal information by the direct marketing industry and to begin a serious and substantive inquiry into the development of appropriate privacy safeguards for consumers in the information age.") *http://www.epic.org/privacy/internet/ftc/ftc-letter.html*. Letter from Senators Bryan, Pressler, and Hollings to FTC Chairman Robert Pitofsky ("We are writing to request that the Federal Trade Commission conduct a study of possible violations of consumer privacy rights by companies that operate computer data bases.") [http://www.epic.org/privacy/databases/ftc-databases.html]

[19] "Office of Information and Privacy Commissioner British Columbia," Table of orders (Last Updated May 13, 1999) [http://www.oipcbc.org/orders/orders-index.html]

1999. Several months after filing our complaint there is no indication at the FTC web site that any action has been taken on the Intel Pentium III matter. Meanwhile, privacy agencies around the globe have begun formal investigations into the Pentium III matter.[20] How can it be that the agency charged with safeguarding privacy in the United States has yet to issue a statement on this matter?

PROBLEMS WITH SAFE HARBOR

Many of the problems with the current approach to privacy protection in the United States can be seen in the ongoing debate with the European Union over the Safe Harbor proposal. That proposal came about in response to the efforts of the European Union to develop a comprehensive privacy policy that would both promote economic growth and protect the privacy rights of citizens in the years ahead. The EU Directive requires that countries which process data on European citizens provide an "adequate" level of privacy protection.[21] Many countries have taken the requirement in the EU Data Directive as an opportunity to update and extend their privacy laws to protect the interests of their citizens.

The United States—at least the Administration—has chosen instead to develop a commercial "safe harbor" that allows US firms to meet the minimal requirements necessary to continue to do business in Europe without actually developing any new laws or rights for US citizens.[22] But even this approach may not succeed. The European Commission working group that represents the privacy interests of European citizens has expressed great concerns about the Safe Harbor proposal. The Privacy Working Group recently issued an opinion on the effort.[23] This is what they had to say:

> Data protection rules only contribute to the protection of individuals to the extent to which they are followed in practice. In an entirely voluntary scheme such as this compliance with the rules must be at least guaranteed by an independent investigative mechanism for complaints and sanctions which must be, on the one hand dissuasive and, on the other give individual compensation where appropriate.

Significantly, the European expert group also said "the standard set by the OECD Guidelines of 1980 cannot be waived as it constitutes a minimum requirement for the acceptance of an adequate level of protection in any third country."

Leading consumer groups in both the United States and Europe have also rejected the safe harbor approach.[24] In a statement issued last month by the Trans Atlantic Consumer Dialogue, representing sixty consumer organizations from across Europe and the United States said that:

> The Safe Harbor proposal now under consideration by the United States and the European Union fails to provide adequate privacy protection for consumers in the United States and Europe. It lacks an effective means of enforcement and redress for privacy violations. It places unreasonable burdens on consumers and unfairly requires European citizens to sacrifice their legal right to pursue privacy complaints through their national authorities. The proposal also fails to ensure that individual consumers will be able to access personal information obtained by businesses.

TACD urged the rejection of the Safe Harbor proposals and recommended instead the development and adoption of an International Convention on Privacy Protection that will help safeguard the privacy interests of consumers and citizens in the twenty-first century.

It is possible that the Safe Harbor proposal will be adopted in some forum by the time of the US–EU Summit in Bonn. But if that comes to pass, a very unfortunate

---

[20] "Working document: Processing of Personal Data on the Internet," Adopted by the Working Party on 23 February 1999 (DG XV 5013/99–WP 16) [http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp16en.htm]; "Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware," Adopted by the Working Party on 23 February 1999 (DG XV 5093/98–WP 17) [http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp17en.htm]

[21] *Privacy Law Sourcebook* 201–27.

[22] [http://www.ita.doc.gov/ecom/menu.htm]

[23] Working Party on the Protection of Individuals with regard to the Processing of Personal Data,, Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999, Adopted 3 May 1999 (5047/99/EN/final WP 19) [http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp19en.htm]

[24] TransAtlantic Consumer Dialogue "Resolution on Safe Harbor Proposal and International Convention on Privacy Protection" (Brussels April 1999)[http://www.tacd.org/meeting1/electronic.html#safe]

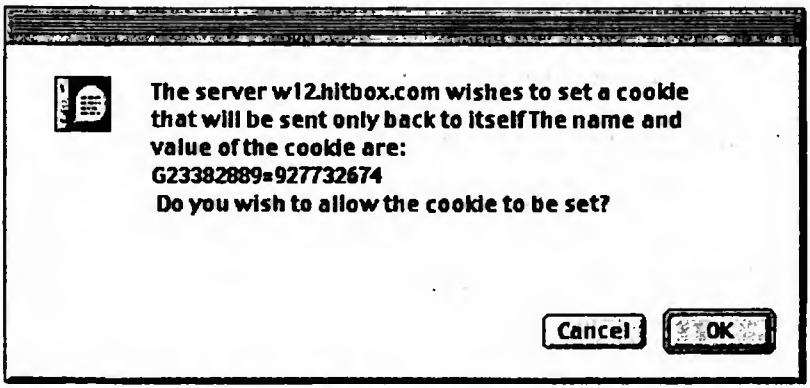
circumstance will result. US firms will offer a higher level of privacy protection for the processing of records on Europeans than they will in processing the records of Americans. This is one of the consequences of a policy that places such little emphasis on the privacy rights of US citizens.

PERSISTENT PRIVACY PROBLEMS AND COOKIES

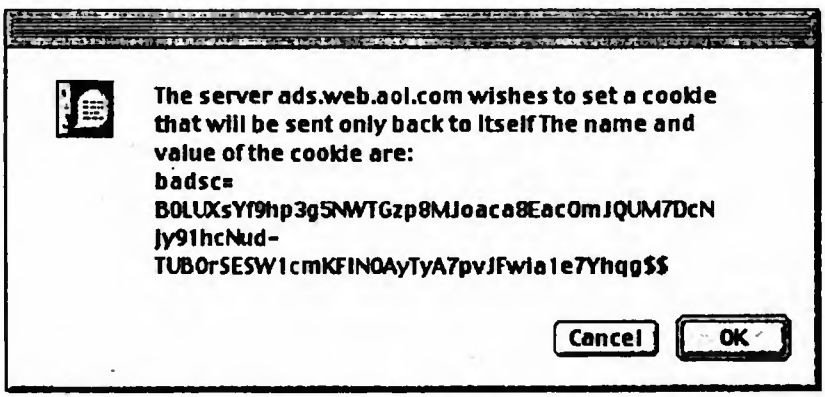
Another area where the failure of the self-regulatory approach can be seen is in the ongoing debate over cookies and other techniques that enable the collection and use of personal information. While it should be said at the outset that cookies perform many useful functions in the online world, it should also be recognized that there are privacy risks associated with the routine tagging of Internet users who visit web sites.

When we looked at the cookies issue in 1997 we said that one of the main problems was the lack of transparency: users could not make meaningful choices about whether to accept cookies because the purpose and use was completely opaque.

How do things stand two years later? To answer that question I was prepared to produce a survey showing that cookie practices were no more helpful today than they were two years ago. Looking at the Top 100 web sites listed in the Online Privacy Alliance survey, I could show for example that a typical cookie notice looks like the following:

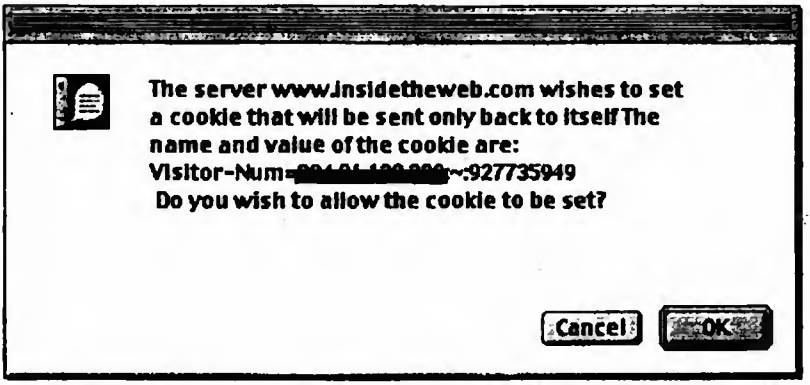



I could even point out that on some cookie files have such a long VALUE field that the user does even get to see the full question:




But as I reviewed the cookies practices at the web sites identified as the TOP 100 in the OPA Survey, I uncovered an even more serious problem. Some of the web sites are using the end-users IP address for the cookie file, which means that if I reprint the cookies statement here you will see my IP address.

Consider the web site; *www.insidetheweb.com*. This is a typical portal site that provides access to other web site grouped by topic area and is supported by advertising revenue. If you go the www.insidetheweb.com site, a cookie notice similar to the following will appear on your screen:




The privacy policy of Insidetheweb states the following:

> We use IP addresses to help diagnose problems with our server, and to administer our Web site. We do not link IP addresses to any personal information such as that provided when registering for a new message board. In rare instances IP addresses may be used to assist in deterring and/or preventing abusive or criminal activity on message boards.
>
> Our site uses cookies to count and track site visits anonymously. A cookie is a small piece of data that many Web sites write to a file on your hard disk. A cookie can contain data like an ID number used to track what pages are visited. A cookie cannot by itself be used by a Web site to obtain personal information about the user or to read information from your computer other than that which has been voluntarily provided by you or is contained in cookies given by the same Web site.[25]

I am not an expert in web protocols but it seems obvious that a cookie that collects a user's IP address is not anonymous. Is this the basis for an action at the FTC? Perhaps. But the better approach, and the approach that will make it easier to avoid an endless parade to the FTC in the years is the enforcement of Fair Information Practices and the development of new techniques to protect online privacy. And the studies that are necessary at this point are the ones that look at the actual practices that web sites follow and not the privacy policies which are often not worth the HTML they're coded in.

## PRIVACY LAWS AND PRIVACY TECHNIQUES

I am very much aware of the important work by members of this Subcommittee and particularly Mr. Goodlatte to promote the widespread availability of strong techniques, such as encryption, to protect the privacy and security of network users and to reduce the risk of crime and network attack. As you may know, EPIC was established in 1994 in the campaign to stop the Clipper encryption scheme, and we very much support your continued efforts to relax export controls.

The interesting question, though, is whether it is more or less difficult to make strong techniques available to protect privacy in countries do not respect the right of privacy in law. While some continue to view privacy techniques as an alternative to privacy laws, I think the better and more accurate view is that privacy techniques and privacy laws are complimentary. Strong encryption is more likely to emerge and be freely used in countries where the legal right of privacy is well established.

The point is clear if you consider the recent history of negotiation over international cryptography policy. The United States government has tried repeatedly to obtain foreign acceptance of the key escrow concept, but such efforts have been resisted in part because of national privacy laws and the European Data Directive,

[25] http://www.insidetheweb.com/privacy.shtml

which make key escrow encryption inherently suspect. Only when the United States had the opportunity to pursue an international negotiation on encryption policy beyond the reach of national privacy authorities was it possible to obtain support for new export limitations on the use of encryption software.

Thus privacy laws and privacy officials turn out to be not only an ally for consumers, citizens, and users but also companies and developers of advanced networked services. Privacy agencies around the globe continue to support the development of genuine privacy enhancing techniques that may in the long term obviate the need for much privacy legislation. Technology professionals also understand that the design and development of information systems means that the responsibility for privacy risks must be carried who are best able to avoid the problem. The Association for Computing Machinery has had a long-standing commitment to privacy protection. The ACM's own code of professional conduct makes clear that it is the developer of systems who must in the end take responsibility for privacy protection.[25]

The lesson here is that if we want good techniques to promote privacy online we will need good laws for online privacy.

## CONCLUSION

I won't pretend that privacy protection in the online world will be easily solved. We are at the beginning of a long and complicated process. We will constantly have to make decisions individually and collectively about how important we believe privacy to be and what steps we are prepared to take. Imagining a comprehensive solution to information privacy in 1999 would be like to trying to imagine how to solve the problem of environmental protection in 1899—many of our greatest challenges lie ahead.

But I do think that more can be done to protect privacy and that Congress will have a significant role to play. There is more than enough precedent in US law and enough ingenuity in the technical community to move us in the right direction and give us at least a fighting chance of protecting what Justice Brandeis called "the most comprehensive of all rights and the right most cherished by a free people.

Key steps will include the following:

- Establish a privacy agency with the expertise, competence and resources to assist consumers, act as ombudsman, and a voice for privacy within the administration
- Promote the establishment and enforcement of Fair Information Practices and encourage the development of simple, predictable uniform rules to protect personal information
- Encourage the development of new techniques that limit or eliminate the collection of personally identifiable information

Perhaps the simplest and least controversial proposal is the Online Privacy Provision contained in Title III of the Internet Growth and Development Act of 1999, HR 1685. This provision would require commercial web site operators that collect personally identifiable information to post a privacy policy and then to treat a violation of the policy as an unfair or deceptive trade practice. This would establish a minimal baseline for privacy in the online world. I do not think it goes far enough, but it is a start.

---

[25] Respect the privacy of others.

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

ACM Code of Ethics and Professional Conduct [http://www.acm.org/constitution/code.html]

The time for surveys has past. If we are to protect privacy, then we must take the necessary steps to ensure that the loss of privacy will not be the cost of the Information Society.

Mr. GOODLATTE. Mr. Berman, welcome.

## STATEMENT OF JERRY BERMAN, PRESIDENT, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. BERMAN. Thank you, Mr. Chairman, members of the committee. It is an honor to be here to talk about the issue of privacy on the Internet. As usual, I am somewhere in between all of the prior speakers. I think that progress has been made; not as much as it should, but progress has been made.

I also take issue with Mr. Rotenberg that the Internet is not making progress relative to other sectors. That growth in Internet policy is being compared against—we have many sectors offline that have no privacy policy whatsoever, and we don't have the numbers to compare, but there are many industries that have zero privacy policies. So it is that kind of comparison.

There is also a problem when you compare the government in the United States on encryption policy with governments overseas. Yes, lots of governments may be for more strong encryption overseas, but they don't have a fourth amendment and fifth amendment and first amendment to deal with this in their country, so their law enforcement's investigative means are more at their disposal. So I don't think that the way to get at this privacy problem is to say that the United States is lagging behind European countries in terms of privacy. The issue is, on all fronts can we do a better job?

You also have to break the issue down into its components. Privacy is not just private data and fair information practices. As you know from moving the issue of encryption, privacy is a complicated and complex issue which involves several expectations of privacy. The first and most important for the consumer is confidentiality in their communications.

The Electronic Communications Privacy Act, which you raised with the government representative here, in our view is broken. It was drafted in 1986 before the Web, before the networking of enormous amounts of information, before America Online had the kind of databases it has, and if you look at a chart that we have done on the protections against government access to information, that is the green, which is stay in your home and your information is fine, the more you move out on the Net, the lower the standards for government access are.

So there has been a revolution in the way we deal with information, and having grown up in the Watergate era, I believe that the major threat to privacy comes from government, and we do not have adequate rules against government.

So do you need legislation? Yes. So the people say we don't need legislation aren't looking at all of the problems. We need legislation against the government to set new standards for privacy on the Internet.

Number two, we need legislation to deal with government. They are the biggest collector of information, and only one-third of their sites have a privacy policy up. They are not using the technologies

like P3P to make them privacy-compliant. They should be in the lead, not behind the private sector in terms of privacy.

And let me get down to the private sector, just a couple of remarks. There is a long way to go from the numbers in the Georgetown study, and I don't see a way that you can get to 100 percent through self-regulation. There is just too many bad actors, too little guidance on the Net. And there is the need to write rules for the road, but they have to be sensitive to those variations on the Net that one size hat fits all, that needing a TrustE or a BBB seal program may be sufficient to comply with privacy. That would help to drive the self-regulatory efforts and not change the direction toward some government agency enforcement.

If we look at legislation, it has to build on the self-regulatory efforts, and we have to answer some hard questions about what it means to access information in the commercial context, what it means to have a real remedy. Those issues need to be answered before we pass legislation. If there is one thing we know, the Internet is complicated, it requires a multitude of new thinking, and we don't want to get it wrong. We got it wrong in the first amendment area and in the content area. We shouldn't get it wrong in the privacy area. We are anxious to work with you to find a solution that moves us forward.

Thank you, sir.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF JERRY BERMAN, PRESIDENT, CENTER FOR DEMOCRACY AND TECHNOLOGY

I. OVERVIEW

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about privacy in the online environment. CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies. We thank the Chairman and Representatives Berman and Goodlatte for holding this hearing and for their commitment to seeking policies that support both civil liberties and a vibrant Internet.

CDT wishes to emphasize three points this morning:

The Internet presents new challenges and opportunities for the protection of privacy. Our policies must be grounded in an understanding of the medium's unique attributes and its unique potential to promote democratic values.

Privacy is a complex value. In the context of this discussion, we believe Congress should focus on ensuring that individuals' long-held expectations of autonomy, fairness, and confidentiality are respected as daily activities move online. These expectations exist vis-à-vis both the public and the private sectors.

By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified.

Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. The concept of fairness is embodied in the Code of Fair Information Practices—long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."[1]

In terms of confidentiality, we need a strong Fourth Amendment in cyberspace. But confidentiality protections—both technical and legal—are growing increasingly porous as technology changes and more information resides outside of the home on networks. It is time to update and strengthen the Electronic Communications Privacy Act. Further, our laws protecting pri-

[1] Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

vacy will have limited impact in the global environment. For that reason, to ensure that citizens and businesses have the ability to protect their sensitive information and communications, the government must change its policy course on encryption.

Preserving these core elements of privacy on the Internet requires a thoughtful, multi-faceted approach combining self-regulatory, technological, and legislative components.

## II. WHAT MAKES THE INTERNET DIFFERENT?

CDT focuses much of its work on the Internet because we believe that it, more than any other medium, has characteristics—architectural, economic, and social—that are uniquely supportive of democratic values. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu.

But while the First Amendment potential of the Internet is clear, and recognized by the Supreme Court, the impact of the Internet on individual privacy is less certain. Will the online environment erode individual privacy—building in national identifiers, tracking devices, and limits on autonomy? Or will it breathe new life into privacy—providing protections for individuals' long held expectations of privacy?

The Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy. However, Anonymizers, anonymous remailers, and other privacy-enhancing tools allow individuals to create zones of privacy—limiting who knows what about them and protecting their sensitive communications from prying eyes. Computer code and products are becoming increasingly critical to the protection of privacy in this distributed environment. With privacy-enhancing tools users will be empowered to control their personal information in new ways.

As we move swiftly toward a world of electronic democracy, electronic commerce and indeed electronic living, it is critical to construct a framework of privacy protection that fits with the unique opportunities and risks posed by the Internet. But as Congress has discovered in its attempts to regulate speech, this medium deserves its own analysis. Laws developed to protect interests in other media should not be blindly imported. To create rules that map onto the Internet, we must fully understand the characteristics of the Internet and their implications for privacy protection. We must also have a shared understanding of what we mean by privacy. Finally we must assess how to best use the various tools we have for implementing policy—law, computer code, industry practices, and public education—to achieve the protections we seek.

### *The Erosion or Privacy and the Path Towards its Restoration*

There are several core "privacy expectations" that individuals have long held vis-à-vis both the government and the private sector, the protection of which should carry over to interactions on the Internet. The remainder of our testimony will discuss the three critical expectations of autonomy, fairness, and confidentiality, explore the changes in technology and policies that threaten them, and finally outline a plan for their restoration.

### *The Expectation of Autonomy*

#### *Why is it at risk?*

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. Online, individuals believe that if they have not affirmatively disclosed information about themselves, then no one knows who they are or what they are doing. But, contrary to this belief, the Internet generates an elaborate trail of data

detailing every stop a person makes. The individual's employer may capture this data trail if she logs on at work, and it is captured by the Web sites the individual visits. This transactional or click stream data can provide a "profile" of an individual's online life.

Two recent examples highlight the manner in which individuals' expectation of autonomy is challenged. (1) The introduction of the Pentium III processor equipped with a unique identifier (Processor Serial Number) threatens to greatly expand the ability of Web sites to surreptitiously track and monitor online behavior. The PSN could become something akin to the Social Security Number of the online world—a number tied inextricably to the individual and used to validate one's identity throughout a range of interactions with the government and the private sector. (2) The Child Online Protection Act (COPA), passed in October, requires Web sites to prohibit minors' access to material considered "harmful to minors." Today, when an individual walks into a convenience store to purchase an adult magazine, they may be asked to show some identification to prove their age. Under the COPA, an individual will be asked not only to show their identification, but also to leave a record of it and their purchase with the online store. Such systems will create records of individuals' First Amendment activities, thereby conditioning adult access to constitutionally protected speech on a disclosure of identity. This poses a Faustian choice to individuals seeking access to information—protect privacy and lose access or exercise First Amendment freedoms and forego privacy.

*The Path to Individual Autonomy Online*

While the global, distributed environment of the Internet raises challenges to our traditional methods of implementing policy, the specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. In the area of autonomy, focusing on standards and applications is crucial. By building systems that respect individuals varied needs for identification, pseudonymity, and anonymity—building a digital wallet with cash, credit cards, a metro fare card, and a driver's license—will help build an online environment that promotes autonomy. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-friendly architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy. Of course, it would also provide individuals the opportunity to create relationships that are identifiable—or at least authenticated—for engaging in activities such as banking. This would be coupled with policies that allow individuals to control when, how, and to whom personal data collected during interactions is used or disclosed.

While there is much work to be done in designing a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in tools like the Anonymizer, Crowds, and Onion Routing, which shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit. Coupled with rules such as those found in the Government Paperwork Elimination Act of 1998, which established privacy protections governing personal information collected when the public uses electronic signature systems,[2] technology may evolve in ways that support individuals' interest in autonomy.

*The Expectation of Fairness and Control Over Personal Information*

*Who controls the data?*

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, cur-

[2] Many such systems gather sensitive information in the course of providing and guaranteeing an electronic signature. The law prohibits companies that collect such information from using or disclosing it without the permission of the person involved. Authored by Senators Leahy and Abraham, this marks the first attempt to craft a legislative approach to dealing with the potential erosion of privacy created by electronic signature use.

rent practices, both offline and online, foil this expectation of privacy. Whether it is medical information, or a record of a book purchased at the bookstore, or information left behind during a Web site visit, information is routinely collected without the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

Focusing on the online environment, we now have information from two studies assessing the state of privacy notices on the World Wide Web. Last June, the Federal Trade Commission's "Privacy Online: A Report to Congress" found that despite increased pressure, businesses operating online continued to collect personal information without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that, while 92% of the sites surveyed were collecting personally identifiable information, only 14% had some kind of disclosure of what they were doing with personal data.

The newly released Georgetown Internet Privacy Policy Survey provides new data. The Survey was designed to provide an update on the state of privacy policies on the World Wide Web. The study shows that definite progress has been made in making many more Web sites privacy-sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. Indeed, fair information practices on the Web appear to remain the exception, not the rule.

The Georgetown Survey shows that, spurred by surveys documenting consumer concern and anxiety, and the work of individual companies[3] and industry self-regulatory entities such as TrustE, the Online Privacy Alliance, and the Better Business Bureau, an increased number of Web sites are providing consumers with *some* information about what personal information is collected (44%), and how that information will be used (52%). Companies posting fuller information about their data handling[4] are more likely to make them accessible to consumers. Many have a link to such statements from the home page (79.7%).[5]

However, on important issues such as access to personal information and the ability to correct inaccurate information, the Georgetown Survey shows that only 22% and 18% respectively of these highly trafficked Web sites provide consumers with notice. On the important issue of providing individuals with the capacity to control the use and disclosure of personal information, the survey finds that 39.5% of these busy Web sites say that consumers can make some decision about whether they are re-contacted for marketing purposes—most likely an "opt-out"—and fewer still, 25%, say they provide consumers with some control over the disclosure of data to third parties.[6]

Overall, the Georgetown survey reveals that, at over 90% of the most frequently trafficked Web sites,[7] consumers are not being adequately informed about how their personal information is handled.[8] At the same time the survey found that over 90% of these same busy consumer-oriented Web sites are collecting personal information.[9] In fact, the survey revealed an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20%), names (up 13.3%), and even Social Security Numbers (up 1.7%).

Thus, while many companies appear to be making an effort to address some privacy concerns, the results from the consumer perspective appear to be a quilt of complex and inconsistent statements. While progress is evident in some areas, the

---

[3] For example, IBM recently stated that it would limit its advertising to Web sites that post privacy notices.

[4] The report calls these "privacy policies" as compared to "information practice statements." "Privacy policies" are a more comprehensive description of a site's practices that are located in a single place and accessible through an icon or hyperlink. A site may have a "privacy policy" by this definition but still not have a privacy policy that meets the elements set out by the FTC or various industry self-regulatory initiatives for an adequate privacy policy.

[5] In response to the question, "Is a Privacy Policy Notice easy to find?" surfers in the 1998 survey answered yes for approximately 1.2% of Web sites. FTC Report, Appendix C Q19.

[6] This number is generated using the data from Q32 (number of sites that say they give consumers choice about having collected information disclosed to outside third parties)—64—and dividing it by 256 (the total survey sample (364) minus the number of sites that affirmatively state they do not disclose data to third-parties (Q29A) (69) and the number of sites that affirmatively state that data is only disclosed in the aggregate (Q30) (39)).

[7] Only 9.5% of the most frequently visited Web sites and 14.7% of those that collect information had privacy policies containing critical information called for by the FTC, the Administration, and required by the Online Privacy Alliance, TrutstE and the BBB Online, about notice; choice; access; security; and contact information.

[8] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices.

[9] 92.9% are collecting some type of personal information.

number of sites that provide consumers with the types of notices required by the Online Privacy Alliance, the Better Business Bureau and TrustE, and called for by the Federal Trade Commission and the Administration, is still relatively small (9.5%).

The posting of privacy notices is not just a private sector issue. In a CDT study of federal agency Web sites, last month, we found that just over one-third of federal agencies had a "privacy notice" link from the agency's home page. Eight other sites had privacy policies that could be found after following a link or two and on 22 of the sites surveyed we could not find a privacy policy at all.

*Establish Rules That Give Individuals Control Over Personal Information During Commercial Interactions*

We must adopt enforceable standards, both self-regulatory and legislative, to ensure that information provided for one purpose is not used or redisclosed for other purposes without the individual's consent. All such efforts should focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare in 1973. The challenge of implementing privacy practices on the Internet is ensuring that they build upon the medium's real-time and interactive nature to foster privacy and that they do not unintentionally impede other beneficial aspects of the medium. Implementing privacy protections on the global and decentralized Internet is a complex task that will require new thinking and innovative approaches.

The Georgetown Survey supports our belief hat a combination of means—self-regulation, technology, and legislation—are required to provide privacy protections on the Internet. The study, as discussed above, shows that some progress has been made in making many more Web sites privacy sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. Because many Web sites need baseline policy guidance and because self-enforcement mechanisms, while emerging, may not always provide a viable remedy, we believe that legislation is both inevitable and necessary to ensure consumers' privacy on the Internet.

To achieve real privacy on the Internet, we will need more than better numbers, redoubled efforts by industry, or a legislative mantra. We will need a good-faith concerted effort by industry, consumer and privacy advocates, and policymakers to develop real and substantive answers to a number of difficult policy issues involving the scope of identifiable information, the workings of consent and access mechanisms, and the structure of effective remedies that protect privacy without adversely affecting the openness and vitality of the Internet.

As the Federal Trade Commission's rulemaking under the Children's Online Privacy Protection Act and industry's various efforts at self-regulation show, these issues are not easy. But armed with the findings of the Georgetown Internet Privacy Policy Survey, we believe interested parties are in a position to move forward on a three pronged approach—expanded self-regulation, work to develop and deploy privacy-enhancing technologies such as P3P, and legislation—all require a serious dialogue on policy and practice options for resolving difficult issues in this promising medium.

In its testimony last July, the Federal Trade Commission stated that, ". . . unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary."[10] Despite the considerable effort of Congress, the Federal Trade Commission, the Administration and industry to encourage and facilitate an effective self-regulatory system to protect consumer privacy, based on the survey results we do not believe that one has yet emerged.

Last year, the Federal Trade Commission offered a legislative outline that embodied a framework, similar to the one we suggest, building upon the strengths of both the self-regulatory and regulatory processes. This year several bills have been introduced on a wide range of privacy issues. Senators Burns and Wyden,[11] and Leahy[12] have introduced proposals as have Representatives Goodlatte and Bou-

[10] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices. *Privacy Online: A Report to Congress*, Federal Trade Commission, June 1998.

[11] The Online Privacy Protection Act of 1999 (S. 809), introduced on April 15, 1999, by Senators Burns (R–MT) and Wyden (D–OR).

[12] Electronic Rights for the Twenty-First Century Act of 1999 (E–RIGHTS) (S. 854), introduced on April 21, 1999 by Senator Leahy (D–VT).

cher,[13] and Vento.[14] We anticipate additional proposals from Senators Kohl, Torricelli, Dewine, and Hatch, and Representative Markey. Historically, for privacy legislation to be successful, it must garner the support of at least a section of the industry. To do so, it generally must build upon the work of some industry members—typically binding bad actors to the rules being followed by industry leaders—or be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act.

Several companies have staked out leadership positions on the issue of online privacy and several self-regulatory programs have formed to drive industry best practices online. Numerous surveys have documented that consumers are concerned about their privacy in e-commerce. In addition, work is underway to develop the tools necessary to implement fair information practices on the World Wide Web. The World Wide Web Consortium's Platform for Privacy Preferences ("P3P") is a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to promote openness about information practices, to encourage Web sites to post privacy policies and to provide individuals with a simple, automated method to make informed decisions. Through settings on their Web browsers, or through other software programs, users will be able to exercise greater control over the use of their personal information. Regardless of how policies are established, an Internet-centric method of communicating about privacy is part of the solution.

As Congress moves forward this year, we look forward to working with you and all interested parties to ensure that fair information practices are incorporated into business practices on the World Wide Web. Both legislation and self-regulation are only as good as the substantive policies they embody. As we said at the start, crafting meaningful privacy protections that map onto the Internet requires us to resolve several critical issues. While consensus exists around at least four general principles (a subset of the Code of Fair Information Practices)—notice of data practices; individual control over the secondary use of data; access to personal information; and, security for data—the specifics of their implementation and the remedies for their violation are just beginning to be explored. We must wrestle with difficult questions: When is information identifiable? How is it accessed? How do we create meaningful and proportionate remedies that address the disclosure of sensitive medical information as well as the disclosure of inaccurate marketing data? For the policy process to successfully move forward these hard issues must be more fully resolved. The leadership of Internet-savvy members of this Committee and others will be critical as we seek to provide workable and effective privacy protections for the Internet.

*C. The Expectation of Confidentiality*

*1. Who has access to records in cyberspace?*

When individuals send email they expect that only the intended recipient will read it. In passing the Electronic Communications Privacy Act in 1986, Congress reaffirmed this expectation. Unfortunately, it is once again in danger.

While United States law provides email the same legal protection as a first class letter, the technology leaves unencrypted email as vulnerable as a postcard. Compared to a letter, an email message is handled by many independent entities and travels in a relatively unpredictable and unregulated environment. To further complicate matters, the email message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the privacy protections are likely to stop at the border.

Email is just one example. Today our diaries, medical records, and confidential documents are more likely to be out in the network than stored in our homes. As our wallets become "e-wallets" housed somewhere out on the Internet rather than in our back-pockets, the confidentiality of our personal information is at risk. The advent of online datebooks, and products such as Novell's "Digital Me", and sites such as Wellmed.com[15] which invite individuals to take advantage of the conven-

[13] Internet Growth and Development Act of 1999 (H.R. 1685), introduced on May 5, 1999 by Representatives Boucher (D–VA) and Goodlatte (R–VA).

[14] Consumer Internet Privacy Protection Act of 1999 (H.R. 313), introduced on January 6, 1999, by Representative Vento (DFL–MN).

[15] WellMed.com is a proprietary Online Health Management System which works by collecting personal health information from individuals, analyzing that information to develop unique health profiles which are used for a variety of purposes. One service is HealthNow!—"an online

Continued

ience of the Internet to manage their lives, financial information, and even medical records raise increasingly complex privacy questions. While the real "me" has Fourth and Fifth Amendment protections from the government, the "Digital Me" is increasingly naked in cyberspace.

*2. Protecting the Privacy of Communications and Information*

Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. The Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored on servers controlled by third parties. Daily interactions such as our choice of articles at a news Web site, our search and purchase of an airline ticket, and our use of an online date book, such as Yahoo's calendar, leave detailed information in the hands of third-parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: 1) the traditional Fourth Amendment standard for records stored on an individual's hard drive or floppy disks; 2) the Title III-Electronic Communications Privacy Act standard for records in transmission; 3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record; and 4) a statutory standard allowing subpoena access and delayed notice for records stored on a remote server, such as the diary of a student stored on a university server, or personal correspondence stored on a corporate server.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

Congress took the first small step towards recognizing the changing nature of transactional data with amendments to the Electronic Communications Privacy Act enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). But the ongoing and accelerating increase in transactional data and the detail it reveals about individuals' lives suggests that these changes are insufficient to protect privacy.

Moreover, the Electronic Communications Privacy Act must be updated to provide a consistent level of protection to communications and information regardless of where they are stored and how long they have been kept. Senator Leahy's recently introduced legislation is an effort to restore 4th Amendment protections to our personal papers. Technologies that invite us to live online will quickly create a pool of personal data with the capacity to reveal an individual's travels, thoughts, purchases, associations, and communications. We must raise the legal protections afforded to this growing body of detailed data regardless of where it resides on the network.

## CONCLUSION

No doubt, privacy on the Internet is in a fragile state. It is clear that our policy framework did not envision the Internet as we know it today, nor did it foresee the pervasive role information technology would play in our daily lives. Our legal framework for protecting individual privacy in electronic communications, while built upon constitutional principles buttressed by statutory protections, reflects the technical and social "givens" of specific moments in history. Crafting privacy protections in the electronic realm has always been a complex endeavor. Reestablishing protections for individuals' privacy in this new environment requires us to focus on both the technical aspects of the Internet and on the practices and policies of those who operate in the online environment.

However, there is new hope for its restoration. There is a special need now for dialogue and action. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. Cooperation among the business community and the nonprofit community is crucial. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or de-

---

personal health record enabling secure, confidential, and private storage, management, and maintenance of health information by individuals and their families. HealthNow affords easy access of medical records from one central location anytime and anywhere the need arises."

veloping legislation—none will happen without a forum for discussion, debate, and deliberation.

The work outlined above, and the state of privacy today, all weighs in favor of creating a privacy entity within the federal government. We believe that the existing, often piecemeal, approach to privacy issues has hindered the development of sound policy and failed to keep pace with changes in technology. Such an entity has important roles to play on both domestic and international fronts. It would serve as the forum for collaboration with other governments, the public interest community, and the business community.

We thank the Committee for the opportunity to share our views and look forward to working with the members and staff and other interested parties to foster privacy protections for the Digital Age.

Mr. GOODLATTE. Thank you all for your excellent testimony.

Ms. Varney, you have outlined the significant improvement in the number of Web sites that post privacy policies. This appears to be an accepted practice by most of the largest Web site operators; wouldn't you agree?

Ms. VARNEY. Yes, I would.

Mr. GOODLATTE. And I notice that you have expressed support, as have a number of others, for the Georgetown study, which uses the standard of policy disclosure as adequate for the protection of privacy. Do you share that view?

Ms. VARNEY. My interpretation of the survey is just slightly different, Mr. Goodlatte. I think that the Georgetown survey did an overall view of how many sites are doing anything, and that gave you the 66 percent number. Then they dove down and they broke it up, how many are doing notice and choice, how many are doing access, and when you go across and say, okay, how many are doing all five, and maybe all five poorly, as Mr. Rotenberg pointed out is possible, that gets you to the 10 percent number. So our goal is to get 100 percent of sites on the Web site to have what I would call robust privacy that meets all five elements in a meaningful way.

Mr. GOODLATTE. So would you say that disclosure is adequate, or would you say that all five is adequate?

Ms. VARNEY. No, I think we need all five.

Mr. GOODLATTE. Thank you.

Mr. Pittman, you want to comment on that?

Mr. PITTMAN. I agree, all five, I agree.

Mr. GOODLATTE. Can you tell me how many of the Web sites that TrustE places its seal of approval on today, how many there are?

Mr. PITTMAN. How many Web sites have the TrustE seal? 675, I believe, is the number.

Mr. GOODLATTE. And how many Web sites use either TrustE or BBB Online; how many of those Web sites that use either one of those two things? What is that percentage of all the Web sites?

Mr. PITTMAN. Of all the Web sites—I don't know about BBB Online. I don't have data on them. As a percentage of all Web sites, I am more inclined to think of it in terms of the percentage of the Web site traffic, because there are millions of sites, and most of them are quite small, personal sites, but a third of the average traffic in any given time is on a TrustE site, I believe is the data we have seen, and as far as on a monthly basis, the percentage of the Web site audience that will visit a TrustE site at least once, the current data from the Georgetown study is about 90 percent. It is very high.

Mr. GOODLATTE. Somebody bent upon misusing information for fraudulent purposes or even for legal purposes, the number, as you cited, millions of Web sites, is a problem in terms of individual consumers getting exposed to misuse of their information or use for purposes they didn't intend or for outright fraud, is a problem that needs to be addressed.

Mr. PITTMAN. I would agree.

Mr. GOODLATTE. And would you agree that many of those who do not post privacy policies online—which we applaud, which we think is outstanding, and we think that the high rate of participation by the larger-traffic Web sites is excellent—but many of those smaller sites that don't post privacy policies online do so for fraudulent reasons or for reasons of taking advantage of information that people on those sites would not be able to utilize?

Mr. PITTMAN. No, I don't think that is the case at all. What I do every day is try to build a Web site business, and it is a challenge to in 18 hours a day to find the slots of time that are required for a start-up company to devote the energy that is required to a comprehensive policy, because all start-ups want to be great big companies 1 day.

Mr. GOODLATTE. When I say many, I don't mean a huge percentage. I mean that out of millions, if you had thousands of sites, that is a very small percentage, but nonetheless a significant danger for consumers on the Web site.

Mr. PITTMAN. It is a significant danger for sites to not have a policy statement and for them to be bad actors.

Mr. GOODLATTE. Okay.

Mr. PITTMAN. I am referring mostly to the media-like qualities of the Web site, which mean that most people visit a smaller number of sites than there ever will be. There are hundreds of cable channels, but most of the viewing occurs on 20 channels. The Web site has similar qualities.

Mr. GOODLATTE. All right. This time I recognize the chairman of the committee.

Mr. COBLE. Thank you. I want to thank you again, Mr. Goodlatte, for having sat in, in view of my circuitous schedule today; and I apologize to the panelists for my not having been here for the entire hearing.

Let me put this question to Messieurs Cerasale, Pittman, Rotenberg and Ms. Lesser. Is government regulation of online practices, including privacy disclosure, incompatible with the technology of the Internet? Mr. Cerasale, let me start with you.

Mr. CERASALE. Incompatible with the technology, probably not, it is not. I think that the potential danger is if you have government regulation which tends to narrow the scope so that future changes in technology may be inhibited is one of the fears of looking at the technology side.

Mr. COBLE. Mr. Pittman.

Mr. PITTMAN. I would agree with that. I am more concerned about inhibiting the growth of the World Wide Web site, which is the new highway that connects consumers and businesses and consumers globally.

Mr. COBLE. Mr. Rotenberg.

Mr. ROTENBERG. Mr. Chairman, not only is it not incompatible to have simple, predictable rules for the Internet in law, it has already been done at least for transborder data flows going back to 1980, and I describe in my testimony in some detail the OECD privacy guidelines which were intended to enable the flow of information across multiple jurisdictions, and the U.S. was a signatory to this.

I also say in my testimony that an interesting question is whether these privacy policies that vary from site to site are incompatible with the nature of the Internet. One of the things that makes the Internet so easy for people to navigate is that they have common reference points and common frames as they move from site to site. If you have to wait for graphics to download, if buttons start moving around, things slow down. Privacy policies are actually slowing down, I think, the ability for online users to move from site to site with privacy assurance.

Mr. COBLE. Ms. Lesser; then I will get to you, Mr. Berman.

Ms. LESSER. I agree with Mr. Cerasale and what Mr. Pittman said about the importance of not slowing down the technology, but I would ask your question in a slightly different way, which is is the Internet fundamentally different than other media. So are we talking about substance or the communications medium itself?

The Internet, of course, is a new medium. It makes data flow; it makes commerce, many communications functionalities much easier. So as we look going forward, what the rules of the road should be, what the role of the private sector is, what the role of government is enforcing against fraud as we heard from the Department of Justice and setting a framework, I think it is hard to answer that question with a simple yes or no.

Mr. COBLE. Mr. Berman, let me put another question, then I will get back to you on this one. Let me put this question to Ms. Varney, Ms. Lesser and Mr. Berman.

More companies are providing some disclosures since last year, which is probably good news, but are companies providing enough options and information for individuals and in a user-friendly manner or operation? Ms. Varney.

Ms. VARNEY. I think the answer, Chairman, is some are and some aren't, and we are continuing to work to get companies to have, you know, easy-to-find and easy-to-read privacy policies. That is our goal. It can't be hard. Consumers have to know right up front what is being done with their information and what are their choices about it. So the idea has taken root.

You know, 2 years ago, 3 years ago, we were around rooms like this saying, huh-uh, people were arguing you didn't have an obligation if you were a company to disclose your privacy or disclose your data practices. That is a foregone conclusion now. We have the obligation. The question is how do we make it easier, and we are still working on it.

Mr. COBLE. Mr. Berman.

Mr. BERMAN. I believe that there are more companies putting out privacy, but there is a very big difference between self-regulation and self-governance. In my view, self-governance is arriving at some social contract about what the rules of the road are. I am not talking about creating a gigantic privacy agency, but to get 100

percent for the rule on the Internet about certain privacy, fundamental rules, fairness, notice, consent, opt-out, some remedy, you need some baseline, and I do not know how to accomplish that without legislation or some self-regulatory program that I have not seen yet, which is the ability to round up the 100 percent and drive it.

I applaud the Online Privacy Alliance, I work with them. I think they are doing a terrific job, but there is going to be a hard problem getting the incentive for the rest of them out there. I think the technology can be very compatible with privacy policies. It is incompatible with the million different kinds of privacy policies that you have to read through, but what Jerry Cerasale at DMA is saying is that there is a possibility if you arrived at this baseline of developing Web site browsing technology that would read those privacies as you went along, and so it would be a seamless experience for the consumer, so the technology is there to make privacy more abundant and clearer on the Internet.

Mr. COBLE. I see my red light is on, Mr. Chairman, so I will back off.

Mr. GOODLATTE. Thank you, Mr. Chairman.

The gentleman from California, Mr. Berman.

Mr. BERMAN OF CALIFORNIA. Thank you, Mr. Chairman, and I apologize once again for missing the testimony, but I am going to take it with me. I think this is a very important subject, and it was only because of the importance of the other subject that I wasn't here. And since I haven't read the testimony, I am going to ask a more general question.

I have been privy to some sort of a general debate about government regulation versus self-regulation, the European model versus the American model. If the regulation model is so good, then how come the Europeans have done so poorly in the context of development of the Internet and in many of these areas of technology vis-a-vis the Americans? And there is a lot of appeal in that argument.

The other side of the coin is when I hear—there is two aspects of the other side, it seems to me. One is everybody is against regulation except for where they are for it. My friends in the content-owner community: No, don't regulate, stay away from all this, except ensure our legal protections against infringing—against mechanisms which will undercut our ability to protect against infringing. The online service providers: No regulation, except please regulate our liability for infringing.

Ironically, some folks in the civil liberties world who stay away from the obscenity, pornography efforts to content regulation, but on the issue of privacy—as you just said, Mr. Berman, I have no idea how we are ever going to get 100 percent compliance with robust protections any more than in society how you are going to get 100 percent compliance with decent norms of social behavior without laws.

And I was told that one of the witnesses talked about this goal of 100 percent robust policy; at the same time—I think it was Ms. Varney—no regulation. It is inconceivable to me that—and, I mean, it is a nice goal, and I have a goal for world peace, but I am not quite ready for unilateral disarmament. But I don't see how you—in this wild world there will always be someone who thinks there

is something to sell, there is some money to be made, and may pay lip service to the robust policy, but in reality we will do something very different.

So that is just some random thoughts, and I would be interested in any of your reactions.

Ms. VARNEY. I will be happy to—or maybe I am not qualified to answer because I am for unilateral disarmament, so I am not sure if my call would be right.

Mr. BERMAN OF CALIFORNIA. See, it is an anarchic world.

Ms. VARNEY. I think, Mr. Berman, your points are extremely well taken, and as many have pointed out, I think the debate between self-regulation and regulation is largely a red herring. If the goal is good, robust privacy online, the question is how do we get there. Now, a number of people at this table have said we need to regulate the collection of information from and about children, period, and we did, and we support that. At the end of the day, maybe we will need regulation around privacy generally.

My view is that right now this is a nascent market. It is moving quickly. There are businesses evolving around the protection of privacy. There are tools evolving around the protection of privacy. I am not always so confident that the government is the best source for me to exercise my rights. Sometimes it is; sometimes it is not. So my whole view is shaped by let's see if we can make this marketplace work with government assistance, and if it doesn't work, well, then we have to go somewhere else.

So my view is that we are not there yet. Moving from 14 percent of sites having some type of disclosure last year to about 66 percent having some type of disclosure this year is enormous progress by anybody's measure. So let's keep moving, keep the pressure on from the government, keep the pressure on from consumer activists, keep responsible businesses in the leadership, and if it doesn't work, at the end of the day I will be the first one up here.

Mr. BERMAN. Maybe we should try and figure out what "keeping the pressure up" means, because even if we could come up with—as I said, in terms of legislation there are some very difficult issues that need to be worked through, and there has never been any privacy legislation; whether it is a video privacy act or ECPA, they didn't have a consensus between privacy advocates and the industry. So until they sit down and put it together and everybody works it out, it is not going to happen.

And I agree with a lot of Ms. Varney's comments, which is that it is nascent industry, but it seems to me just in terms of the pressure on, the online privacy alliance is driving, BBB's driving, but the government can put pressure.

It seems to me ridiculous that the industry should have had to come up with the shekels to pay for the study of where their compliance is. Why doesn't the FTC have enough money from the Congress to conduct a real study in January and have another benchmark, see where everyone is in terms of the five elements? Are we up from 60 to a 100 percent? Has anyone gone from the 10 percent real compliance upwards? Fund that study and maybe get the FTC or somebody to bring people together and deal with these hard issues, what is a remedy, what do we mean by identifiable information on the Internet, how do we use technology, and to frame some

recommendations so that it is not just a dialogue about where we are, but have some concrete things for you to look at.

I certainly don't want to send this off to a 2-year privacy protection study commission, but there is some short-term kinds of efforts that could be prodded by government and which need to be, because the Catch-22 about the Internet is that we are against big government regulations. Don't create an FCC, don't create it for the Internet, don't create a big agency. Great, but then how do you get the Internet to get together? What process exists so that they can engage in self-governance?

So someone has to convene and bring together—you know, everyone went to Philadelphia to draft the self-regulatory Articles of Confederation. It has to be done by something, and I think government has to be the prod.

Mr. ROTENBERG. Mr. Berman, if I may say, I think you are absolutely onto the critical point in this debate. I mean, people don't want to be regulated. They want others to be regulated for their benefit, and one of the frustrations in the privacy community is that in so many areas, whether it is copyright protection or content, you know, we are out in front, passing new laws, creating commissions, but in the privacy area, we remain committed to self-regulation.

I think the corollary is that regulation is not necessarily the goal either. The goal, as I said in my statement, is privacy protection. Now, if you take privacy protection as your goal, you begin to realize a number of things. You may be able to achieve it in part through some industry leadership. You may be able to achieve it in part through some legislation that establishes baseline privacy rights. You may be able to achieve it in part by creating some type of privacy agency that gives direction and oversight to whatever privacy policies and principles you are trying to put in place. Those are the building blocks of a privacy policy, of a program that says we are committed to protecting this right of privacy on into the next century, we want to take advantage of these new technologies, we are excited about the Internet, but we don't think our ticket for admission, if you will, should be our personal privacy.

The problem is we don't have those building blocks in place today. We are so committed to trying to show that self-regulation can work. People are saying, let's put baseline legislation on hold, let's not create a new agency, let's give self-regulation some more time. We have given it a lot of time, and we know from experience that it will not provide the type of protection and the type of assurance that I think people in this country are entitled to. The right of privacy, the concept of protecting right of privacy in law, comes from the United States, and those privacy laws, privacy rules that Europe is trying to say to the U.S., "where are they today?" started here. So I think we have some catching up to do.

Mr. BERMAN. May I respond?

Just one of the problems with the debate between the privacy advocates and industry policymakers is that sometimes the privacy advocates are not very clear by what they mean by privacy. They say we need a benchmark, we need a rule, we need a set of compliance. The Europeans have got it, but getting the privacy community to play the card, which is to put the card on the table about

what is the minimum, what is the basic, what will get somebody some applause up on the Hill or in the press or in industry that they have done a good job, what is the minimum—because the tendency is always to define it and then to play the game of move the line so that whatever anyone does, it doesn't meet the real test of the privacy community, and that is turning politics into religion, and I don't think it is a very good way to accomplish anything.

Mr. PITTMAN. Excuse me, I am sorry.

Mr. GOODLATTE. Go ahead very quickly.

Mr. PITTMAN. I just wanted to contribute a couple of comments from where the rubber meets the road. My experience is in start-up companies and then the largest at the time, 1996, ISP, Internet provider, Netcom. I joined the company to start their online advertising, an e-commerce program. I had experience in the direct marketing world and believed, based on what I knew there, that we could apply a lot of that technology to marketing on the Web site.

I ran into a brick wall, and that was the perceived policy issue; went to TrustE, which was being formed at the time, and we completely dropped that program not because it was illegal, but because we decided it would put us out of business. We would have such a flood of e-mail and such a flight of customers, it would not be tenable to launch a program like that.

We very quickly got the religion that this is a different business, this is a different world. It was very difficult to sell within Netcom and within our general counsel the idea of signing a policy with a seal program. That should have been our responsibility to speak, and we were using a third party to do that. But eventually they accepted that, and then we wrote it into our contracts with our third parties so that we wouldn't do business with companies who didn't have policies. And now in a start-up I have just joined, which has eight people, we want to be a $100 million company in a couple of years.

But it is part of our culture, it is part of our business, it is part of the way we will do business, and all I can say is that is something that is going on in Silicon Valley and in this business, and it is very important. I am not saying that regulation is not necessary, but that is powerful, and that has happened in 3 short years.

Mr. GOODLATTE. Thank you.

The gentlewoman from California.

Ms. LOFGREN. Thank you, Mr. Chairman.

I think this has been very helpful. I am not sure what we are going to end up doing, but this has been a very useful discussion.

In reading through the written testimony, one of the questions I had, Marc Rotenberg, was about your remarks on page 9 of your testimony. You and Mr. Berman talked about anonymity. This is the first time I ever heard the word pseudonymity. I kind of like the concept as an approach to online privacy. You mention that the German government adopted legislation to encourage the use of anonymity for commercial sites. What did they do to encourage it?

Mr. ROTENBERG. I appreciate the question, Congresswoman. Their 1997 multimedia law, which was an effort to try to establish legal framework for the Internet and other new forms of communication, also took on the challenge of trying to update the privacy

laws, and they said that the basic privacy laws were good, and they wanted to carry them forward.

They also said the Internet offers new opportunity to protect privacy by reducing the collection of personal information. If we reduce the collection of personal information, we also reduce the regulatory burden. I mean, if businesses get paid, and people get products and services, the privacy problem goes away, which I think everyone agrees would be a great thing. So they said, in law, let's encourage our online services to make payment schemes available that allow for anonymous transactions.

It is that kind of productive prodding that recognizes the advantages of new technology to protect privacy that can also be done in cooperation with business, and I think it is terribly unfair to people who are working to protect privacy in this country to view us simply as pushing for government regulation.

We have been on the front lines with the business community pushing for the availability of the very best techniques to protect privacy, but it is not just about encryption, it is not just about export controls. It is about techniques for anonymity, ways to protect identity, and to protect privacy while minimizing risk.

Mr. BERMAN. We agree with everything that Marc just said. There are several expectations of privacy, including anonymity, the ability to be able to shop and browse and go around the Internet without being identified. We expect that in our lives, and we want to take that into the virtual world, everything from pseudonyms and encryption, and we need to look at the authentication issue.

I also think that we need legislation. As a privacy organization I am up here saying we need legislation to deal with government access, to update ECPA and to even maybe export ECPA to the rest of the world.

In the private sector data world, I think we need legislation to set a baseline, but I think that we have to have a good faith effort to work that out and to address some hard issues and to find a process, and I think that the most imaginative thing that the Congress could come up with is a process that brings people of good faith from privacy community on my side, and Marc, and the consumers, and AOL, and the DMA, and the policy people from the Hill and the administration to the table.

Ms. LOFGREN. Let me ask you a question, Mr. Berman. On your testimony, on page 6 and 7 you talk about the architecture of the Internet, which I think is important for us to focus on. I am not sure where it leads us ultimately, but the privacy-enhancing architecture needs to be incorporated. What role, if any, should the Federal Government play in supporting or nurturing or encouraging that?

Mr. BERMAN. One thing that it could do, there is a technology that doesn't articulate a privacy policy, but it creates a privacy language for the Web which can express what the policies of a Web site are to your browser and also allows a consumer to state their preferences and deal only with sites which they agree with. That is an interesting——

Ms. LOFGREN. So this would be part of the architecture.

Mr. BERMAN. That is part of the architecture.

Ms. LOFGREN. It would avoid the problem of your zipping through the sites when you don't ever actually get to articulate your preferences.

Mr. BERMAN. Your browser is going to read it, and we have been working on that with a lot of other people.

One of the other things to do is make the government compliant. One of the things that the government tried to do in the encryption area is when they came up with a wonderful idea of escrowed funds is to have the government be the purchaser. Well, why doesn't the government become P3P—which is the technology—compliant, so that anyone going from the IRS or to the government can read privacy policies.

Ms. LOFGREN. Let me frame my remarks in terms of the architecture where the browser communicates and establishes the policy. I believe a lot of people online don't have any idea how little privacy there is. If they did, they would quickly get off line. If there were more information available to the public about, generally, what is a cookie. I think that would make a difference. I have told some Members of Congress how a cookie works and they say, "You are kidding!" It is a stunning revelation to people who are new to it. If there were a market for such technology, would the government have to play any role in this at all?

Mr. BERMAN. No. I think that there is a—it is very interesting that in the obscenity area you have got 100 and some odd tools out there being developed by people to block sites that people don't like because they don't like the content, but the consumer movement has not come up with any kind of—I mean, I will tell you, Marc's campaign against the Intel chip, there has been no consumer response about how to figure out tools, and on the Internet—maybe Marc wants that—that educates consumers about which sites have privacy policies and create a market incentive for sites to comply with policy or consumers aren't going to go there because the browser is taking them somewhere else.

Mr. GOODLATTE. Go ahead quickly, and then we must move on.

Mr. ROTENBERG. Thank you.

Just a couple of brief comments. First of all, we do at our Web site make available privacy tools that is on a page that is called Practical Privacy Tools—encryption, everything else.

Secondly, I want to say I think the idea of having the government become P3P-compliant is nutty. The government is subject to the Privacy Act. It is a law that establishes basic privacy rights for all citizens. It is not something that you express a preference about, and it is not something that the government can say, "you know, the FAA is at 50 percent of the Privacy Act, or the Department of Commerce is at 75 percent of the Privacy Act."

I think one of the problems we are seeing, and this is a reflection of the effort to promote self-regulation, is that a lot of these new techniques don't actually protect privacy. P3P, for example, which takes as a presumption that preferences are good and a one-size-fits-all solution is bad, has been under development for several years now, and I think what they are finding paradoxically is that many different sizes turns out to fit no one, because what people want on the Internet are simple, predictable, uniform rules. They

want their privacy protected, and they want to enjoy the Internet. They don't want to spend their time reading privacy policies.

Ms. LESSER. Can I just add one thing, and that is to say I think this discussion about, you know, is the market pushing toward technological development and pushing toward privacy policies is not one we should be having in an aspirational way. I think, indeed, it is important for efforts to go on to educate consumers about what they should be demanding, but as a company that serves 18 million members, I will tell you this is a market issue. It is a market issue. When we make mistakes, we hear from an incredible number of people because it is easy for them to complain to us. When we don't offer privacy policies that are easy to understand, easy to find, we hear from our members, and we implement those policies in coordination with our business partners. So it is important to look at this issue in the context of what is going on in the market right now.

I believe that AOL and other companies have seen a huge increase in e-commerce in part because we have seen a huge increase in efforts toward trust, and so as we begin this dialogue, I think it is a dialogue that we have to have with privacy advocates, with you folks up here, within the administration, with people around the world. We do recognize the current market, the current market pressures which we feel every single day.

Mr. GOODLATTE. Thank you.

We will now recognize the very patient gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. I really don't have any questions, Mr. Chairman. I think this is very informative and very instructive and fascinating really. I don't know if the gentlelady wants more time, but I will be happy to yield to her.

Mr. GOODLATTE. We are going to do another round.

Mr. DELAHUNT. I would just make an observation that after listening, I do see a confluence of interests here. I think Ms. Varney made the point, and I think Mr. Berman made the point. I mean, I think if you are going to be successful, the American consumer has an overarching interest in privacy.

And I remember the ill-fated attempt by an agency to enact the so-called Know Your Customer rules. My office was deluged with complaints. And the fact that we do have legislation kicking around might be a mechanism to ensure—I think it was Ms. Varney's term—robust privacy, because I think that Congress is poised to act. I can't say that I am really conversant with the volume of documented violations of privacy, but I am clearly familiar with some of them.

It was good testimony. It was a very good hearing. Thank you. I yield back.

Mr. GOODLATTE. I thank the gentleman.

I really must say I think the gentleman from California hit the nail on the head here in—and a number of you have acknowledged that. At some point in time, we may need to do something to reach out and get those—the gentleman has pointed out that on virtually any issue we confront on the Internet the issue is not whether we have absolutely no government involvement or total government involvement but finding the appropriate balance.

And so, Mr. Cerasale, I would like to ask you, since Mr. Varney and Mr. Pittman acknowledged at some point in time we may need to have some of this, don't you agree that we can't reach those bad actors, those folks who are just not going to adhere to any voluntary standard with some kind of a base standard, whether it be simply saying that what the industry standard has evolved will apply to everybody or something to impose that?

Mr. CERASALE. Well, I think in the end it may be that we have to look toward government to try and get some baseline.

I think that there is another potential approach. If we have good education of consumers that here are privacy policies that you must follow, and the privacy policies are out there and have consumers look for those privacy policies, and we have some form of self——

Mr. GOODLATTE. Mr. Rotenberg pointed out when someone visits the web they may visit 20 or 30 or 40 sites in an hour or two on the Internet. Are they going to each one of the site's policy and make that determination before they proceed further in or are they going to simply skip from one to the other and forget where they have looked and where they haven't looked and have somebody's cookie pick up a whole lot of information they didn't realize somewhere in the process?

Mr. CERASALE. That is true. That is why you have seal programs, so that you don't have to go look. You can look at TRUSTe, you can look at BB on-line, those types of things, and the B—3B program where you could have a seamless communication to come in.

But I do think that if consumers understand and know, they are going to avoid sites that don't have a policy; and then if a site puts up a policy, the true bad guy puts up a policy to get you to come to the site and then violates it, then you have current law that you can go after them, both on criminal and even on the civil side of being a deceptive act in section 5.

Now, it may very well be that we have to go forward further to get government regulation, but it is not—I don't think it is just the right time right at the moment.

Mr. GOODLATTE. That is quite all right.

Ms. VARNEY. Mr. Goodlatte, inherent in the question is the tension between the good guys who are doing the right thing and the bad guys and the vast middle. I think what we saw in 1994 when the Congress passed the Telecommunications Fraud Act, it didn't stop the bad guys. There is more telecommunications fraud today than there was in 1994 when the law was passed. What it did was it gave law enforcement additional tools to prosecute bad guys.

Now, the question of whether or not we need additional tools to prosecute bad guys I think is a fair one. My own view is, as a former Federal Trade Commissioner, is that we have the tools we need to prosecute bad guys.

Mr. GOODLATTE. Could you agree with Mr. Berman that ECPA is broken?

Ms. VARNEY. I am not well enough informed on ECPA to have an opinion one way or the other, but I agree with Mr. Berman on most things, so I will give my proxy on that.

The question of how we get the bad guys I don't think is a question of passing a new law. They are still going to break the law.

They still need to be apprehended, prosecuted and preferably put in jail. The middle, how do you get the sites that are collecting personal data to post their privacy policies I think is the challenge. And what we have seen is that today there has been some progress, enormous progress thus far.

Is it the right time for the government to intervene in that flow? I just don't think it is yet. We have done it for kids. You may do it for medical. You may do it for financial. But for general commercial, I am not sure it is the right time for it.

I think it is a very good point, and timing is absolutely critical here because we have a number of forces converging on the Congress right now. One of those is the increasing public awareness and concerns cited by Mr. Rotenberg, a number of examples of abuses.

The second is the negotiations going on right now with the European Union where they have taken a totally contrary approach, which I have been outspoken in opposition to, which basically starts with the premise that you don't get anything unless you get the consumer's approval, that you are getting it ahead of time, and that government regulation prevails and self-regulation is an afterthought, if at all.

That is an approach that we don't like. But we are in very strenuous negotiations on that. There is going to be a product that comes out of those negotiations, and there then may be tremendous pressure on the Congress to adopt that product as the law of the land.

Mr. GOODLATTE. Would it in your opinion make some sense to be anticipating the pressure that is going to be built and to look at the policy of looking at industry self-regulation and setting that as a standard that those people in the middle that you point out would also comply with?

Let me ask you that—to you, to you and Mr. Cerasale and Ms. Lesser as well.

Ms. VARNEY. I think, Congressman, that the European situation is exceedingly complex. And you know the fact that it is not much discussed—as I think everybody at this table can acknowledge, the European data directive was drafted and written before there was a ubiquitous Internet and certainly before there was a worldwide web. So now we have a situation where we have a bureaucratically-based view about data that was designed before there was a web.

There is a difference, I think, when you look at those businesses whose sole business is the collection, aggregation, sale of information about individuals, and that is where they make their money, is collecting individual data and moving it around the world, as opposed to businesses on the web that may or may not collect personal information and may or may not have any use other than fulfilling the transaction or personalizing the website further. So you have got some inherent tensions.

I think we are a very long way from figuring out how this European directive is going to impact us. To tell you, just very briefly, my husband runs a small E-commerce business, hopefully some day to be large, a member of TRUSTe, a good privacy policy. We don't do business in Europe. We don't. And when we get an order from a European, sorry, we don't do business in Europe, because

the costs for us of registering with the data protection registrars in Europe are too high. You know, we make our business here.

Mr. GOODLATTE. That may well be part of their intent.

Ms. VARNEY. But I think that the political process in Europe, where we have many, many friends in France and Britain—you know, when you get a message from my husband's site that says, sorry, we can't do business there because we can't afford right now to comply with your data protection requirements, I think some of those people go back to their governments and say, wait a minute, you know, we want to do business over there. We want to avail ourselves of the goods and services that are available from the United States.

Mr. GOODLATTE. Sure. I would hope that the pressures work both ways. But the pressures are going to exist here to address this in some fashion, and what the Congress has to consider is not only what level of regulation—there are a number of bills that have been introduced in the Congress that I find go much further than I would like to see occur—but we also have to address this issue of timing, because we are going to face the pressure from the public if they feel they are not protected on the Internet.

We have an incentive to address this just as industry does. Industry's incentive is to promote the ability to do business and to draw people on the Internet to conduct that business.

So we respect what you are trying to do and very much support it, but whether it is universal enough is the issue we have to address.

Mr. Cerasale.

Mr. CERASALE. Yes, I think we have been—you are correct. The European directive and how it is applied is going to put some pressure here. Part of the negotiations have been looking at a safe harbor, looking at how industry uses self-regulation and that be accepted in Europe so that we can do business across border.

I think it is important from our perspective to think about the bureaucratic nature of what is happening in Europe, and we clearly don't want that to come about in the United States.

And our personal view—I mean, our view at the DMA, my personal view also, but that doesn't matter much—our view at the DMA is that we are willing—we want to go forward with BDP online, TRUSTe, our own privacy promise, the idea of trying to meet the needs of consumers to give consumers empowerment.

I think the key for us in the Internet is if the consumers feel empowered, therefore, they can control is what is going to increase, vastly increase, our Internet business. That is what we want to encourage and not get bogged down in the government, registration, et cetera, all of that bureaucratic nature that we find in Europe. So we have been really pushing our Commerce Department to go forward with a safe harbor idea. That may or may not come about.

But I think, from our perspective, the view to you is don't make us Europe. There was a revolution. There is a reason not to be there.

Mr. GOODLATTE. Well, I fully agree with that. But the question is, how do you avoid getting there? If you wait too long and the pressures of those who would like to see us have much more significant regulation, a government agency involved in setting all of

these standards and principles, then you are put in a position of having choices that you would not like to have. Whereas if you take the initiative of getting everybody cooperating now and using a minimal standard to say you have got to do these basic minimal things, you have, in my opinion, gone a long way to preempting that.

Ms. Lesser.

Ms. LESSER. I am going to build on what Ms. Varney and Mr. Cerasale said. I agree with a lot what they have said, but I would say this in answer to your question about what you can do. I think that the safe harbor discussions that are going on right now in the Department of Commerce are critical for U.S. industry to be able to comply with, as Ms. Varney said, a law that is I believe outdated and not reflective of the needs of the on-line community.

But having said that, we need——

Mr. GOODLATTE. But it is reflective of the general philosophy that the government will regulate more than we want to regulate here.

Ms. LESSER. To the extent that we are doing business in Europe, we need to comply with that law. So the efforts going on to make sure that compliance with the laws in Europe is made sort of sane for U.S. industry, given our approach to privacy here, I think is critical.

Having said that, there will be a lot of pressure on, I think, the folks up here to address these issues, given those discussions, and we have said so at the Department of Commerce. And I don't think that the answer is that you should say, well, it is not time yet. I think what you have to do is to take those negotiations and then say, well, what standards should apply? Let us set a baseline and start a discussion for what privacy needs to look like in this country. And that I think includes a lot of the things that Mr. Berman, that we, that Mr. Rotenberg have talked about. What are the building blocks of privacy?

I don't think we are going to get an answer this summer. But I do think it is critical, and AOL is anxious to engage in that dialogue. So the answer with the outcome of the safe harbor is begin a dialogue up here and help industry and consumers and everybody get together to find out what the baseline is.

Mr. GOODLATTE. I have been around tables like that before and on-line service provider liability.

Mr. Rotenberg, do you want to respond to that?

Mr. ROTENBERG. If I can just make a comment about that.

Mr. GOODLATTE. That took 3 years.

Mr. ROTENBERG. About the EU directive, I am not going to defend all aspects of the directive; and I understand your concern about the European approach to legislating this area.

I will point out that the EU directive takes up less space in my privacy law source book than will the Children's On-line Privacy Protection Act and the accompanying regulations from the FTC. Because it turns out in the United States it is a much more elaborate and complicated procedure, when you get done legislating and regulating, than it is in the European Commission; and they are very sensitive, I think, to this problem of not slowing down new technology.

But my key point, and really what much of my written statement at the beginning talks about, the significant common ground that existed on this issue 20 years ago between the United States, Europe and East Asia over simple privacy policies—there were eight principles that the OECD set out, the U.S. agreed to, 100 leading companies said we liked, and many of our laws, many of the European laws, the directive, financial practices in Japan and around the world followed those policies.

I think the absolute best advice I can give to you today, without going into how much do we regulate or self-regulate, is to try to find a path back to the OECD guidelines. Figure out to how to implement them and how to enforce them, make them minimally burdensome. But that is the common ground.

Mr. GOODLATTE. Mr. Berman. And then we will go to Mr. Berman.

Mr. BERMAN. My last comment is that I think that we ought to find a path, and one of the reasons why I think that the consideration of legislation is important in this area, when I mean baseline legislation, it may not pass this year, but a real serious effort to try and address the building block pieces of that and what it entails and what the different safe harbors are, that involves the Congress in a very serious way, rather than a comeback next year, is that you begin to develop a policy consensus that doesn't just include the administration but it includes the consumer and the legislature. And that is unless you reach that consensus, you cannot deal with the European directive in a coherent way without a United States consensus. And part of that should be driven by what we have tried to do in other areas, which is to make the regulatory framework sensitive to the unique characteristics of this new medium versus anything else.

Mr. GOODLATTE. Thank you.

The gentleman from California.

Mr. BERMAN OF CALIFORNIA. I had one specific question and one more general question.

There has been reference to safe harbor here. Is this the safe harbor that allows a company to do business in Europe because they comply with the directive? What does safe harbor mean, if you can talk about safe harbor.

Ms. LESSER. There are discussions going on between Ambassador Aaron at the Department of Commerce and the European Commission to determine a way that U.S. companies who are doing business in Europe and want to transfer data back to the U.S. can essentially make an announcement that they are complying with European law so that there won't be any interruption in data flow.

The way the European directives works, some countries will require an adequacy determination and a permission, essentially, before the data can be transferred back to the U.S.

Mr. BERMAN OF CALIFORNIA. But this is not a U.S. decision then, it is a European decision?

Ms. LESSER. It is an ongoing dialogue between the Department of Commerce here and the European Commission. And once the member states theoretically agree we would then have a process where we would—and there are a number of ways we might have to do this, but some of the discussions on the table will be, for ex-

ample, send a letter to the European Commission, say, as the directive obligations are laid out in the safe harbor, there have been negotiated principles. We comply with those principles and, therefore, should be allowed to continue data flows back from Europe to the U.S.

Mr. ROTENBERG. Maybe I can just say a little more directly. Safe harbor is a set of principles that the U.S. has proposed that U.S. companies would agree to follow which would allow Europeans to transfer data to the United States even though it might be said that the U.S. otherwise lacks adequate privacy protections.

So it is, in effect, our alternative in the commercial world to having new privacy legislation. We say our firms will agree to follow these policies to protect the privacy of the European citizens and in the negotiation focus on the adequacy of those policies.

Mr. BERMAN OF CALIFORNIA. So it is self-regulation in order to comply with European regulation?

Mr. ROTENBERG. Exactly.

Ms. LESSER. Exactly.

Mr. CERASALE. Yes.

Mr. BERMAN OF CALIFORNIA. Did any of you touch on the question of—in all of this talk about privacy, are there significant numbers of real people who really care? What I mean is, is the immunization—I have to admit that I do not call for a sweep of my phones every morning before I start getting on them, even though I say a lot of things that I wouldn't want my enemies, the government, my friends, particularly, to hear me saying.

I get immunized a little bit to all of this stuff. In the Internet, there is a little bit of a depersonalized aspect of the Internet where the blush factor doesn't exist. No one quite sees you in that chat room. Do people—is this something that a lot of people, particularly those "legally trained," are focused on but the mass public really doesn't care too much about? I don't care who knows where I shop. I will care, in the same sense that John Boehner cares a little bit more now about privacy in communications by virtue of being a victim. Anybody who has become a victim of a phoney credit card thing or something like that where their privacy was invaded might care, but before that happens people don't care too much.

Mr. ROTENBERG. Privacy is a very funny issue. I can tell you that we get calls in our office every day from people on various privacy concerns, but one of the things that I realized about this issue is you don't really understand how important privacy is until you lose it. I mean, that is one of those things that you think about very abstractly: Oh, I could imagine that this could happen to me, or did you see this story about what happened to someone else? But once someone else gets ahold of your credit card information or once someone else leaks a medical record or something else about you, you feel very strongly.

And I think one of the problems then with this self-regulatory approach is we are taking the attitude, let us see if we have enough damage before we actually legislate; and I don't think that is the best way to do things.

I think it would be better to say, let us see if we can reduce the risk of those privacy violations so people don't have to worry about it. But when it happens to you, you will know it.

Mr. BERMAN. I have one thought on that, too. I think a lot of people believe that they have—that there is a very strong privacy regime in the United States, that they take it for granted. They may care about privacy, but they think it is there for bank records, for medical records. When they hear about the fact that—when they find out that there isn't any or that those standards have disappeared, that may be, you know, when waiting for what Marc calls, you know, the bad actors or the bad examples, then people turn around and say, well, how did that happen? How did we get into a situation where we didn't have the laws, we didn't have the text, we didn't have the regime there? And that is, I think, what the issue is.

Mr. PITTMAN. I think what the net does, it teaches two things at least to consumers who spend time on it. One is how to be more thrifty. They decide that they can find better values if they search. And the other thing it teaches them is that their information has value, has intrinsic value, and they never really thought of it in those terms until they began to bargain with it on the net. I think it is a cultural experience that if you spend time on-line you begin to acknowledge.

Mr. CERASALE. It is also, in thinking about the credit cards, I mean, using the credit card falsely, there are a lot of laws. But do people think about it? Yes, they do.

Thirteen years ago, for example, L.L. Bean had a toll-free number, but 95 percent of their orders came in through the mail, because people—I am dating myself here—were afraid to give their credit card number over the telephone to some strange person they didn't see.

The switch in L. L. Bean—I will throw out what is happening on the Internet. The switch in L. L. Bean now is that 97 percent of their orders come in through the toll-free number, and 3 percent come in through the mail. So there was—clearly, Americans were, back then, looking at the telephone skeptically, worried about security of their financial information. I think it is totally true today.

And as you go through and work on it, they will see and gain confidence in it, and that is an important factor. So the vast middle does care, as it has at least for 13 years.

Ms. VARNEY. I think part of your question was, or as I heard it, does anybody besides the six of you in America care about this in terms of——

Mr. BERMAN OF CALIFORNIA. And those of us here.

Ms. VARNEY. Anybody besides the people in this room. I think the answer is, the empirical evidence as you go narrower and narrower is harder to come by, but there really is a lot of evidence that people who are both on the net and not on the net have a lot of issues around something that is more broadly called trust, and that encompasses security of credit card transactions.

I think it goes to what Mrs. Lofgren said. If people knew the level of data that could be collected about them without their knowledge and consent, they probably would be more concerned. But my own anecdotal evidence tells me that people are cautious about being on the net for a number of reasons. It is not just the articulation of what we would define more narrowly role as privacy. It is part of a larger trust issue.

Ms. LESSER. I will just add one thing, and that is that I think that it really depends on how you ask the question and what you are asking. So the research that we have is that people very much do care, that they understand what we are doing with their information, that we give them choices, that we tell them what kind of security information we do—we give them, that we tell them how they can maintain the accuracy of their information. But—and that is why we have a strong privacy policy.

But when we ask them what they want from the on-line world, they want increased personalization, they want increased interactivity, and they understand that, for example, in order to get increased personalization that they will give up some of their personal information in order for us to give them that service. But they want to have that conversation: Do you have a privacy policy and are you doing what you saying you are doing? But I also want to take advantage of this new medium; and, therefore, I am willing to give up some of my personal information.

Mr. GOODLATTE. Do you have any additional questions, Ms. Lofgren?

Ms. LOFGREN. Just a couple observations.

We are not dealing with a clean slate. We are, however, neatly at the beginning of what it means to be on-line. What we do now is very important. It is going to set the stage for the next century. Maybe it is worthwhile to step back from the little bitty steps that we have taken so far to think, if we were starting almost completely anew about what we are going to do.

It seems to me that we ought to think about what it is that Americans, as this institution is the U.S. Congress, expect as their own personal space. I think most Americans expect the right to be left alone. That is kind of a very American feeling. Individuals have the right not to have other people knowing all kinds of things about them. That is an American thing: I get to be by myself. My neighbors don't have to know everything about me, let alone the government or big companies.

If that is American, what do we need to do to preserve it, or put it in place?

I think maybe one idea that may be helpful here is that the data about me and about you, you own, and no one else owns it. If it is collected about you, it belongs to you. If it belongs to you, then people who take it from you, whether they use it or not, have exposure, perhaps some liability. If you have liability, then you don't need a regulatory scheme, because you will have compliance to avoid liability.

When it comes to the Internet and the worldwide web, the answer almost is always technological. Statutes don't seem to work in an Internet world.

I talked to some Europeans familiar with this problem, along with my colleague, Mr. Goodlatte. It was very interesting. One of the comments made was we are doing all sorts of stuff but we are waiting upon you Americans, because whatever you do is the way it is going to be. This is an interesting perspective. We are the gorilla. Where we sit is where the net is going to be—at least in the short term.

I think, if we just set some clear standards, attach some liability, then the technology will be developed to avoid the liability. In this way, I think we may avoid a regulatory scheme, and, in the bargain, we will meet the expectations of the American people. This also transports our American values to the rest of the world.

And I think, as I have listened to you today, it has helped me crystallized that understanding. For this, I thank you very much.

Mr. GOODLATTE. Thank you. I think that is an excellent note on which to close, and I want to thank all of our panelists for your participation. I would encourage you to continue the excellent dialogue we have had today, and I think we are making some progress in figuring out where we are going on this issue.

So thank you all, and this concludes the oversight hearing on electronic communication privacy policy disclosure. The record will remain open for 1 week. We thank you all for your cooperation, and the subcommittee stands adjourned.

[Whereupon, at 12:32 p.m., the subcommittee was adjourned.]

# APPENDIX

## MATERIAL SUBMITTED FOR THE HEARING RECORD

INTERNET CONSUMERS ORGANIZATION,
*Chevy Chase, MD, May 28, 1999.*

Hon. HOWARD COBLE, *Chairman,*
*Subcommittee on Courts and Intellectual Property,*
*Committee on the Judiciary,*
*House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: I am submitting the attached statement for the record of your hearing on May 27, 1999, with the hope that it provides a difference perspective on privacy, especially privacy in an online electronic environment.

The Internet Consumers Organization (ICO) has recently been formed to provide policymakers and other interested parties with fair and balanced positions on issues of importance to both Internet consumers and providers of online services. Our objective is to help shape a progressive environment for the Internet, and to conduct research and education programs that enhance consumer confidence in using the Internet for e-commerce and other purposes. ICO is in the process of filing for nonprofit status. ICO has not received any federal grant, contract or subcontract.

Thank you for considering our views.

Sincerely,

PETER GRAY, *ICO Co-Founder.*

PREPARED STATEMENT OF PETER GRAY, CO-FOUNDER, INTERNET CONSUMERS ORGANIZATION (ICO)

CONSUMER PRIVACY—ASSUMPTIONS VS REALITY

In the privacy arena, the rationale for public policy appears to be based on a series of assumptions that rely heavily on: public attitude polls; media exposure of abuses; potential threats to personal privacy; and the European Data Protection Directive.

Let's examine 10 key assumptions about privacy, especially online privacy, and compare them to the reality of the marketplace.

1. Assumption: Consumers are universally concerned about the privacy of their personal information.

Reality: Some people are more privacy-sensitive than others; some care most about protecting only sensitive information, like medical records; others don't seem to care, and are willing to trade off some or all of their privacy for lower cost or other benefits.

2. Assumption: Consumers who say they are concerned about their privacy will refrain from using the Internet.

Reality: People often behave or act differently from what they say or believe. This is a form of cognitive dissonance that may explain the discrepancy between the Harris polls, where 81% of Net consumers say they are concerned about privacy, and the explosive growth in Internet usage. What's really happening? The Pew Research Center found that Americans' daily Internet usage rose from 4% in 1995 to 25% in 1998. The Department of Commerce forecasts 250 million Internet users next year and over a billion during the next decade.

3. Assumption: Privacy concerns are keeping consumers who use the Internet away from using e-commerce.

Reality: The facts don't bear this out. Forrester Research estimates that 26% of online users made regular purchases on the Web last year. Jupiter Communications found that the number of people buying something on the Net grew from I0MM in 1997 to 17MM last year. Examples: Priceline and E-Trade attracted over a million online customers in less than a year.

4. Assumption: Most consumers are worried about unauthorized access to their e-mail messages.

Reality: Forrester Research shows that 89% of online users regularly send e-mail-still the most frequent use of the Internet. Most of these users are not worried about the privacy of their e-mails. People who are concerned about e-mail privacy can use anonymous identities, encrypt their messages or refrain from sending confidential information via e-mail.

5. Assumption: Consumers consider Internet privacy as more important than convenience, security, reliability, cost, value, choices, customer service, speed of access and other benefits.

Reality: Some may, others may not. People have a hierarchy of needs and preferences, which may change. Someone shopping for the lowest cost airfare available may be willing to divulge a degree of personal information in order to get the ticket. Someone else who pays bills online may value security and reliability of the service more highly than privacy. Researchers surfing the Web may be primarily interested in speed of access.

6. Assumption: Consumers will not do business with companies that don't have have privacy policies or privacy seals posted on their websites;

Reality: Most people want to deal with companies that they trust and have confidence in. Good privacy policies and practices are one element of trust. Customer service,, dispute resolution, product quality and other factors are also important elements of trust.

7. Assumption: Consumers trust governments over businesses to protect their privacy.

Reality: Not necessarily. Notable privacy lapses by the IRS, SSA, state MV bureaus, health care and other agencies certainly don't engender public trust that their personal information is being kept confidential. In addition, U.S. consumers views may differ from those of other nationalities.

8. Assumption: Consumers need government laws and regulations to protect Internet privacy.

Reality: Legislation may be necessary 'in some specific instances (eg to cure abuses like identity theft, protect sensitive medical records from unauthorized access). But legislation or regulation is not the panacea for general online privacy protection.

9. Assumption: People have no control over their personal privacy in cyberspace, and they are powerless to protect themselves.

Reality: Consumers have the ability to control their online privacy and they have demonstrated this by public complaints and exposure of privacy abuses or threats (eg CVS, Intel, FDIC). Privacy sensitive consumers refuse to provide certain information about themselves, or may provide incorrect information to companies they don't trust.

10. Assumption: People object to company practices that involve the collection and use of personal information about them.

Reality: A recent Vanderbilt University study reported that over 72% of Web users would provide personal information to companies that disclose how the information would be used. If a company with a good privacy policy discloses it to the public, and uses information it collects to provide consumers with benefits, consumers, are more likely to allow such information to be used to suggest products or services based on their personal preferences. A good example is Amazon.com.

In sum, we need to critically examine and reexamine the assumptions that drive and shape privacy policy in the U.S. and globally and be willing to adapt to a rapidly changing e-commerce market.

THE NAMED INC.,
*Washington, DC, May 27, 1999.*

Hon. HOWARD COBLE, *Chairman,*
*Subcommittee on Courts and Intellectual Property,*
*Committee on the Judiciary,*
*House of Representatives, Washington, DC.*

On behalf of The NAMED Inc., a non-profit privacy group based in Washington D.C., I would like to submit the following statement for the record of the Subcommittee 5/27 oversight hearing on Electronic Communication Privacy Policy Disclosure.

I participated as a member of the advisory committee to Professor Mary Culnan of Georgetown University, who recently conducted two surveys—one for the Federal Trade Commission (FTC) and one for the Online Privacy Alliance (OPA), an industry group. The FTC survey measured certain information practices for the 7,500 most visited consumer sites and the OPA survey measured the same practices for the 100 most visited consumer sites. The full reports of these surveys are available at http://www.msb.edu/faculty/culnanm/gippshome.html.

The NAMED would like to highlight the fact that, according to these surveys, *the default privacy practices of the top 100 sites are WORSE than those of the top 7,500 sites.* When measuring how sites handle the personal information of consumers who do not actively set their privacy preferences, the larger sites demonstrated worse privacy practices in every aspect except security.

The top 100 sites collect more personal information from consumers in 13 out of 16 categories observed (Fax Number, Education and Preferences are the exceptions). They are more likely to use the collected information for marketing or other secondary purposes (83% of those who post policies said that they may do so vs. 73% of the top 7,500 according to question Q27). They are significantly more likely to disclose consumer information to third parties (74% vs. 54% according to Q29), but less likely to commit that such disclosure will only take place in an aggregate non-identifiable manner (27% compared to 30.5% of top 7,500 according to Q30). In their only apparent advantage, the top 100 are more likely to provide proactive security to personal information before/after the collection (46.8%/28.7% vs. 44.3%/18.6%).

These results do not appear to be accidental. The visible posting of privacy policies hides an increasing use of consumer information without permission. Since most consumers probably accept the default settings provided by sites, their privacy on large sites is more compromised than on small ones.

These findings strengthen the position of The NAMED that the only viable solution to privacy is to ban all unauthorized commercial use of personal information.

Sincerely,

RAM AVRAHAMI, *Director.*

---

AMERICAN INSTITUTE OF CERTIFIED
PUBLIC ACCOUNTANTS (AICPA),
*Washington, DC, June 2, 1999.*

Hon. HOWARD COBLE, *Chairman,*
*Subcommittee on Courts and Intellectual Property,*
*Committee on the Judiciary,*
*House of Representatives, Washington, DC.*

DEAR CHAIRMAN COBLE: I am writing to you in your capacity as a Chairman of the Subcommittee on Courts and Intellectual Property of the House Judiciary Committee.

Last week, your subcommittee heard from witnesses on electronic communication privacy policy disclosure. The American Institute of Certified Public Accountants expressed a desire to appear at the hearing to inform the subcommittee of CPA WebTrust—an exciting attest service the CPA's are offering in the U.S. and throughout the world to ensure consumer safety in electronic commerce. Unfortunately, the witness list was completely full and we must communicate through this letter.

Enclosed are some materials we would have provided you at the hearing. We have requested that we be allowed to insert the enclosed statement into the hearing record.

We are excited about WebTrust. In our considered opinion, it provides some needed assurance that consumers can trust the vendors they encounter on the Internet.

If you or your staff have any questions about WebTrust or would like more information about the service, please call me at (202) 434–9205 at your earliest convenience.

Sincerely,

J. THOMAS HIGGINBOTHAM.

PREPARED STATEMENT OF ALAN W. ANDERSON, SENIOR VICE PRESIDENT, TECHNICAL SERVICES AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA)

SUMMARY

There are significant barriers to the growth of electronic commerce that reflect consumer concerns about the risks of doing business on the Internet. Consumers ask questions like:

- How do I know whom I am conducting a transaction with?
- Will I receive what I ordered in the condition that I expect?
- Is it a reliable business?
- Is it a secure site?
- Will my privacy be protected?
- Will I get scammed?

The Internet provides an exceptional opportunity for consumers to conduct business transactions efficiently and effectively in cyberspace. There are various projections for overall growth of such business from about $1.0 billion today to more than $100 billion in the next five to eight years. For these projections to become a reality, the above consumer concerns have to first be addressed.

The CPA profession, through the American Institute of Certified Public Accountants, has researched concerns about electronic commerce and believes the CPA profession is uniquely positioned to offer a comprehensive private sector response to these issues (in essence consumer protection) on the Internet. In response to this need, the AICPA, together with the Canadian Institute of Chartered Accountants (CICA) has developed a new service called *CPA WebTrust*, that is designed to build consumer trust and confidence in the electronic marketplace.

*CPA WebTrust* requires a Web site to:

- disclose its business and information privacy practices and to follow those practices,
- maintain effective controls over the integrity of transactions, and
- Maintain effective controls to protect private customer information.

After a specially licensed CPA has conducted an independent and objective examination of a Web site and determined that the sight has complied with the *WebTrust* Criteria, the Web site can obtain and display the *CPA WebTrust* seal of assurance. However, the process doesn't end there. *CPA WebTrust* requires ongoing periodic updates to ensure that the Web site continues to comply with the *WebTrust* Criteria.

We believe this new symbol of trust is a model for a private sector initiative that will both enhance e-commerce success on the Internet for businesses large and small and also provide for consumer protection. *CPA WebTrust* provides full, fair, and honest disclosure and provides assurance to customers or potential customers that a business engaging in electronic commerce is legitimate and has appropriate controls to protect a customer's interests.

This will allow the customer or potential customer to make informed decisions about doing business on the Internet. Many legitimate businesses will be required to "raise the bar" for doing business with customers on the Internet in order to qualify for *CPA WebTrust* but in so doing, will lay the foundation for future sustainable growth through the establishment of sound business practices and policies

INTRODUCTION

My name is Alan Anderson and I am representing the more than 330,000 Certified Public Accountants in the United States that are members of the American Institute of Certified Public Accountants (AICPA) in my capacity as a Senior Vice President for Technical Services of the AICPA. I am also a former partner of McGladrey & Pullen LLP, a public accounting firm for which I worked over 17 years.

In my testimony today, I will outline the needs of customers in the electronic commerce marketplace, the steps that the CPA profession is taking to provide assurance to customers regarding these needs, and how these initiatives are postured to provide a private sector response to the associated consumer protection needs.

Although I represent the AICPA today, I wish to point out that e-commerce is a global initiative. The service that I will describe is the result of a joint effort between the AICPA and its counterpart in Canada, the CICA, and has been recently licensed to similar accounting organizations in England, Scotland, Ireland, Australia and New Zealand. We anticipate more expansion in the global marketplace in the coming months. For purposes of this statement, references to the AICPA also generally include our international partners.

ELECTRONIC COMMERCE MARKETPLACE AND BARRIERS TO CONSUMER ACCEPTANCE

There have been many projections of the potential growth of consumer-oriented business on the Internet. These are generally in the range of $1.0 to $3.0 billion (less than 1% of total retail sales) today to over $100 billion in five to eight years. These same studies often cite the consumer's concern about the need for protection related to the legitimacy of on-line business and the privacy and security of their transactions and use of personal information. As a result, many studies indicate that only about 20 to 25% of on-line users are willing to complete a purchase transaction over the Internet. As the Internet develops and matures, its success will therefore depend on gaining and maintaining the trust of consumers. This trust will be especially critical to the success of small businesses that engage in electronic commerce and depend on consumer confidence in place of the name recognition or tremendous financial resources familiar to larger businesses.

In order to understand the views of online users toward purchasing products on the Internet, the AICPA commissioned Yankelovich Partners to conduct a survey in mid-1997. This survey, conducted among 1,003 Americans who are 18 years old or older and subscribe to an online service either at home or at school indicated that:

- On-line users are receptive to buying a variety of products over the Internet but often do not do so because of security fears.
  - A large majority of on-line users say they would not provide information about their income (91%) or give out their credit card number (85%) when shopping on-line.
  - Large majorities are even hesitant to provide their phone number (74%) or address (67%).
- A lack of security is the number one reason given by non-buyers for not purchasing products on-line.
- Having credible assurance about the security of on-line transactions would greatly increase on-line purchasing of products and services.

This research indicated that there was a need to build consumer trust and confidence in order to overcome these barriers and for electronic commerce to reach its full potential.

The Yankelovich survey also explored these consumers' views about the concept of *CPA WebTrust*, which was then under development by the AICPA. The survey indicated that:

- More than three-quarters of on-line users have a favorable impression of CPA WebTrust.
- Significantly, nearly half (46%) of on-line users say the *CPA WebTrust* seal would make them more likely to purchase products and services on-line.
- The fact that CPAs are providing this seal of assurance is a key factor in creating user acceptance of *CPA WebTrust*.
- A majority of on-line users—particularly those currently or most likely to shop on-line—say CPA endorsement makes this service more trustworthy, useful, and important.

These findings were reaffirmed by similar research results that were released earlier this year by Ernst & Young LLP, in "The Second Annual Ernst & Young Internet Shopping Study".

ROLE OF THE CPA PROFESSION

For over 100 years, the objectivity and integrity of the CPA has played a major role in shaping the U.S. economy. Consider the development of the U.S. securities market. Without question, the U.S. capital markets are the most effective and efficient in the world. One key element of the efficiencies this market enjoys is the audited financial statements reported on by the CPA.

With the advent of the Securities Acts of 1933 and 1934 and the requirement for audited financial statements to supplement the sale of securities, the CPA stepped

in to fill a void in the capital market place. Because of the independence, integrity and objectivity that a CPA brings to an audit engagement, public confidence in the securities market grew - and continues to grow. Investors learned that an independent and objective professional had examined the financial statements of the seller. The investor could now rely with confidence on the financial information included within a prospectus. This reliability has freed the investor to focus more clearly on assessing management's ability to grow shareholder value.

A strong parallel between the Internet and the development of the securities market exists today. In many respects, electronic commerce on the Internet is in its infancy. The potential economic benefits of electronic commerce have yet to be realized by both retailers and consumers alike.

One reason for this is the lack of trust and confidence consumers have about the Internet. How do I know whom I am transacting with? Is this a reputable company that I can depend on? Is the Internet reliable? Is it secure? These are just several of the questions in potential customers' minds.

To increase consumer confidence and to address these fears and concerns, the AICPA has developed and is offering the *CPA WebTrust* service, with its sister Institutes across the world. In simple terms, Web sites can elect to be audited by public accounting firms and CPAs, who are specifically licensed by the AICPA. Those Web sites that demonstrate they meet all of the *WebTrust* Principles and Criteria are awarded the right to display the *CPA WebTrust* seal of assurance.

The *CPA WebTrust* seal of assurance is a symbolic representation of a CPA's unqualified report, which also appears on the Web site. [Please refer to Appendix A for an example of what a customer will see as he or she views and clicks on the *CPA WebTrust* Seal.]

## THE WEBTRUST PRINCIPLES AND HOW WEBTRUST WORKS

### *The WebTrust Principles*

CPA WebTrust is based on three main principles designed to ensure that Web site operators institute practices to protect consumer interests, while at the same time providing businesses with the tools necessary to stimulate future growth and sustainability on the Internet. Web site management must make a written assertion that their Web site follows these principles. These principles are described as follows.

*Business Practices & Information Privacy Disclosures Principle*

*The entity discloses its business and information privacy practices for electronic commerce transactions and executes transactions in accordance with its disclosed business and information privacy practices.*

To enhance customer confidence in electronic commerce, it is important that the customer is informed about the entity's business and privacy practices for electronic commerce transactions. As a result, it is required for the business to properly disclose its business practices for dealing with such matters as the following:

- A description of the goods or services being offered
- The time frame for completion of transactions
- Method of delivery of goods or services, including customer options
- Payment terms
- Electronic settlement practices and related charges to customers
- Product return policies
- How to obtain customer service and support
- How to file claims, ask questions or register complaints
- How to file a complaint for resolution by a third party using binding arbitration
- How information being collected is being used, maintained or distributed to others,

This principle relates not only to the electronic commerce transaction processes that the business uses, but also provides assurance to a potential customer that the business has a proven history of demonstrating compliance with these disclosures.

WebTrust does not include any direct representation as to the quality of its goods or services nor their suitability for any customer's intended purpose (such matters are outside the scope of the *WebTrust* Principles and Criteria. However, they are covered, in part, in the *WebTrust* Consumer Recourse Mechanism provided through a third party binding arbitration feature).

*Transaction Integrity Principle*

*The entity maintains effective controls to provide reasonable assurance that customers' orders placed using electronic commerce are completed and billed as agreed.*

These controls and practices address matters such as appropriate transaction identification, transaction validation, the accuracy, completeness, and timeliness of transaction processing and related billings, the disclosure of terms and billing elements and, if applicable, electronic settlement. These matters are important to promote confidence in electronic commerce and effectively demonstrate to a potential customer a business's ability to deliver on its sales promise. This demonstrated ability serves to increase sales for the business owner engaging in electronic commerce by reducing the consumer's fear in dealing with the anonymity associated with Internet shopping

*Information Protection Principle*

*The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business.*

These controls address matters such as:

- The collection and use of customer data and a customer's access to such data
- Encrypting private customer information (such as credit card numbers and personal and financial information) transmitted to the entity over the Internet,
- Protecting such information once it reaches the entity,
- Requesting permission of customers to use their information for purposes other than those related to the entity's business, and
- Obtaining customer per-mission before storing, altering, or copying information on the customer's computer.

Consumer concern about the safeguarding of private information traditionally has been one of the most significant deterrents to undertaking electronic commerce transactions.

*The WebTrust Criteria*

In order to provide more specific guidance on meeting the *WebTrust* Principles, the *WebTrust* Criteria have been developed. These criteria provide an objective basis and a consistent set of measurement criteria for CPAs to use in testing and evaluating Web sites and an effective benchmark for a business to use in developing a sound electronic commerce business. The business must be able to demonstrate over a period of time, at least two months and typically three months or more, that (1) it actually executed transactions in accordance with the business and information privacy practices it discloses for electronic commerce transactions, (2) its controls were operationally effective, (3) it maintains a control environment that is conducive to reliable business practice disclosures and effective controls, and (4) it maintains monitoring procedures to ensure that such business practices remain current and such controls remain effective. These concepts are an integral part of the *WebTrust* Criteria. The full text of the *CPA WebTrust* Principles and Criteria document is available at the AICPA's Web site at *www.aicpa.org*.

*The CPA WebTrust Examination*

*Obtaining the Seal*

To obtain the *CPA WebTrust* seal of assurance, an on-line business must meet all the *WebTrust* Principles as measured by the *WebTrust* Criteria associated with each of these principles. In addition, the entity must (1) engage a CPA who has been specifically licensed by the AICPA to provide the *CPA WebTrust* service and (2) obtain an unqualified report from such CPA.

In order to award the *CPA WebTrust* seal, the CPA must examine the Web site in accordance with professional standards established by the AICPA. Those standards require that the CPA plan and perform the examination in such a manner as to obtain reasonable assurance that management's assertion is not materially misstated.

The CPA tests management's assertion that its Web site meets *all* of the *WebTrust* Principles and Criteria. The CPA's examination will include: (1) obtaining an understanding of a business's electronic commerce business and information privacy practices and its controls over the processing of electronic commerce trans-

actions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as are considered necessary in the circumstances.

In many respects, the standards a CPA must follow in performing a *CPA WebTrust* engagement are similar to those followed in performing an audit of financial statements. Both types of engagements require the same planning, supervision and due professional care. In addition, CPAs use a screening process for new clients that ensures that they are legitimate businesses and have a history of meeting their commitments.

Independence and objectivity are two other key elements of both the audit and the *CPA WebTrust* engagement. For example, a CPA cannot have a financial interest in a business that he or she is examining for the *CPA WebTrust* seal. It is these two characteristics that provide a great deal of value to both users of financial statements and the *CPA WebTrust* seal of assurance. Because the CPA has no interest in the business under examination, he or she can make fair and objective assessments of the controls and procedures that management has in place.

*Keeping the Seal*

Once the seal is obtained, the business will be able to continue displaying it on its Web site provided:

- Its CPA updates his or her assurance examination of the assertion on a regular basis. The interval between such updates will depend on matters such as:
  - The nature and complexity of the business's operation,
  - The frequency of significant changes to its Web site,
  - The relative effectiveness of the business's monitoring and change management controls for ensuring continued conformity with the *WebTrust* Criteria as such changes are made, and
  - The CPA's professional judgment.

    For example, an update will be required more frequently for a financial institution's fast-changing Web site for securities transactions than for an on-line service that sells archival information using a Web site that rarely changes.
  - In no event would the interval between updates exceed 3 months and this interval often may be considerably shorter.
- During the period between updates, the on-line business informs the CPA of any significant changes in its business policies, practices, processes, and controls if such changes might affect the business's ability to continue meeting the *WebTrust* Principles and Criteria, or the manner in which they are met. Such changes may trigger the need for an assurance update or, in some cases, removal of the seal until an update examination by the CPA can be made. If the CPA becomes aware of such a change in circumstances, he or she would determine whether an update examination would need to be performed and whether the seal would need to be removed until the update examination was completed and the updated auditor's report is issued.

*Protecting the Seal*

The AICPA has teamed with VeriSign, Inc., a leading provider of digital authentication and security services on the Internet, to provide protection for the *CPA WebTrust* seal. VeriSign conducts an independent verification to ensure that the Web site is a genuine site for the named business and provides a highly secure digital certificate verify the site's identity and protect the *CPA WebTrust* seal.

HOW CPA WEBTRUST HELPS PROTECT A CUSTOMER'S INTERESTS WHILE STIMULATING GROWTH FOR BUSINESSES

We believe that *CPA WebTrust* will help protect the consumer in the following ways:

- Required disclosure of business practices provides significant information for the consumer on which to base purchasing decisions. Our research with business owners displaying the *CPA WebTrust* seal has shown that a reliable form of disclosure on business practices coupled with the assurance of knowing that these practices have a demonstrated history of being followed significantly reduces the amount of time needed to educate potential customers who request information through e-mail or telephone calls. One small business displaying the *CPA WebTrust* seal has reported to the AICPA that it experienced

a significant increase in sales followed the posting of the *WebTrust* seal to its web site.

- Required controls over transaction integrity and information protection help ensure that the risks of doing business over the Internet are minimized. Obviously, this perceived risk by the customer is greater when doing business with an unrecognizable entity.
- For Web sites who do not currently meet the *CPA WebTrust* criteria, the "bar will be raised" for doing business on the Web thereby laying the foundation for businesses to be able to grow and stay a viable force on the Internet.
- Independent verification by the respected CPA profession helps build consumer trust and confidence especially since this is updated at least once every three months. Increased trust and confidence will undoubtedly benefit businesses.
- The CPA and VeriSign both verify the legitimacy of the business and that the business owner's Web site is genuine. This provides reasonable assurance that only legitimate Web sites qualify for the *CPA WebTrust* seal.
- VeriSign provides a digital certificate to protect the *CPA WebTrust* seal and also uses so called "spider technology" to scan the Internet for any sites displaying a WebTrust-like seal without authorization. Attempts to counterfeit the *CPA WebTrust* seal would be quickly detected.
- The AICPA requires CPAs to attend training and obtain a special license in order to provide the *CPA WebTrust* service. As part of the license, the CPA firm agrees to an independent quality inspection of its *CPA WebTrust* services. Most CPA firms have been in the business of providing valuable audit, tax and consulting services to small businesses for decades.

*CPA WebTrust* protects American consumers who shop at overseas Web sites and at the same time, provides trust and confidence to the overseas shopper looking to conduct commerce at the web site of a business in the United States. Because the Internet is global, the AICPA has licensed similar accountant's institutes in a number of countries to offer *WebTrust* as a service to their members.

IN CONCLUSION

Although still in its infancy, electronic commerce shows extremely high potential for our economy and will undoubtedly be of huge benefit to businesses given the relatively low cost of entry. It provides convenience and promotes efficient markets therefore stimulating economic growth. No doubt there will be both intentional abuses and unintentional errors affecting consumers and therefore decreasing trust in this new medium. However, we believe that, if its use becomes wide spread, *CPA WebTrust* will enhance consumer protection on the Internet, and will build the consumer trust and confidence that is needed for electronic commerce to achieve its full potential.

It is our goal that consumers around the world will look to those sites with the *CPA WebTrust* seal as the safe places to shop on the Internet. We believe *CPA WebTrust* will help to create a level playing field for those businesses that don't otherwise have name recognition or the resources necessary to create high visibility in the marketplace. Although Web sites that do not initially qualify for *CPA WebTrust* will need to make the necessary changes to their electronic commerce business practices to meet the *WebTrust* Principles and Criteria, we believe in the long run, that this will better position them for growth and sustainability on the Internet by providing a framework as to how sound electronic commerce is conducted.

We also believe that *CPA WebTrust* is an excellent model for implementing consumer protection and privacy in the private sector.

I would like to thank the Subcommittee for allowing me to submit this testimony for the record.

ALAN W. ANDERSON, CPA, SENIOR VICE PRESIDENT, TECHNICAL SERVICES, AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA)

Mr. Anderson's role at the AICPA includes responsibility for all technical aspects of the CPA profession, including the development of technical standards and the profession's self-regulatory activities. He also oversees the AICPA's Personal Financial Planning (PFP) Division, Tax Division, Industry and Management Accounting Division, Management Consulting Services (MCS) Division, Information Technology Division, and the Partnering for CPA Practice Success (PCPS) Section.

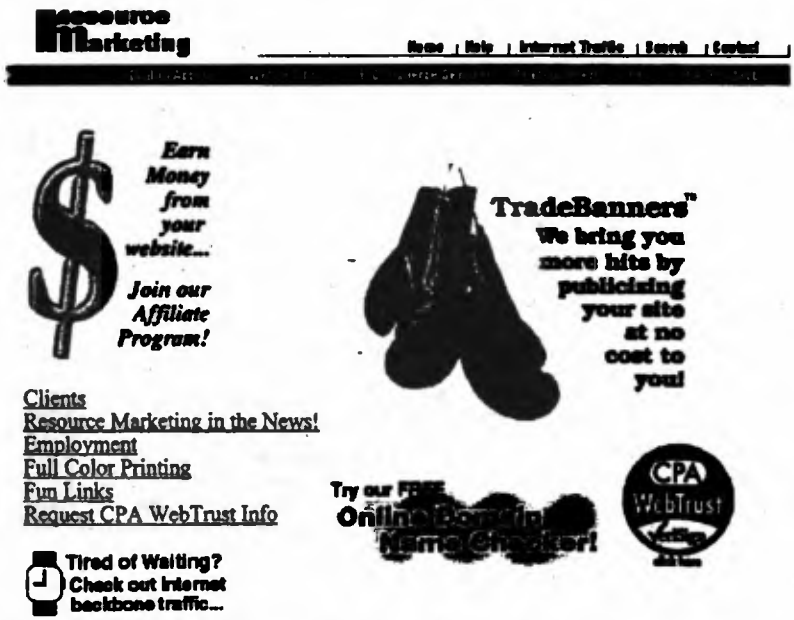
Mr. Anderson also has responsibility for the AICPA's initiative on expanded assurance services for the CPA profession, which includes the *CPA WebTrust* program.

He is a member of the AICPA, the Minnesota Society of CPAs, and the Information Systems Audit and Control Association.

Prior to joining the AICPA in November 1996, Mr. Anderson was a line partner and the national director of audit with the CPA firm of McGladrey and Pullen, LLP (Minneapolis, Minnesota), where he gained over seventeen years of experience in audit, control and security matters with some of the firm's largest clients in a variety of industries.

# Appendix

# A


Resource Marketing
Earn Money from your website...
Join our Affiliate Program!
TradeBanners™
We bring you more hits by publicizing your site at no cost to you!
Clients
Resource Marketing in the News!
Employment
Full Color Printing
Fun Links
Request CPA WebTrust Info
Try our FREE
CPA
WebTrust
Tired of Waiting?
Check out Internet backbone traffic...
TrustCart™ – the easy way to add E-commerce!


CPA WebTrust Site
The CPA WebTrust seal symbolizes that this site has been examined by an independent certified public accountant who has issued a report on management's assertion that its disclosed business practices for electronic commerce transactions, customer's orders and billing, and controls over protection of customer information were in conformity with the WebTrust Criteria.
The authenticity of the CPA WebTrust seal is provided through Digital ID technology provided by VeriSign, Inc. This site's Digital ID should be verified to verify the authenticity of the CPA WebTrust seal. This can be verified by clicking the button below.
CPA WebTrust
VeriSign
Management's Assertions
Business Practices Disclosures
Independent Accountant's Report
WebTrust Principles and Criteria
VeriSign Digital ID Authentication
INDEX TO SITES WITH THE WEBTRUST SEAL
ADDITIONAL INFO ABOUT WEBTRUST

## Management Assertions

Resource Marketing, Inc. on its Web site for electronic commerce (at resource-marketing.com) asserts the following:

**We have disclosed our business practices for electronic commerce transactions and executed transactions in accordance with these disclosed business practices,**

**We have maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and**

**We have maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to our business**

**during the period January 1, 1998 through February 28, 1999 in conformity with the AICPA/CICA WebTrust Criteria.**

RESOURCE MARKETING, INC.

By: Christopher Swainhart, President

FLEMING,
BROCKSCHMIDT
& DURKIN PLL
Certified Public Accountants

# Independent Accountants' Report

To the Management of Resource Marketing, Inc.:

We have examined the assertion by the management of Resource Marketing, Inc. that "on its Web site for electronic commerce (at resource-marketing.com) during the period January 1, 1998 through February 28, 1999, Resource Marketing, Inc.:

- **disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,**
- **maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and**
- **maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to Resource Marketing Inc.'s business in conformity with the AICPA/CICA WebTrust Criteria." Resource Marketing Inc.'s management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.**

Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance that management's assertion is not materially misstated. Our examination included (1) obtaining an understanding of Resource Marketing Inc.'s electronic commerce business practices and its controls over the processing of electronic commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with disclosed business practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Also, projections of any evaluation of controls to future periods are subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, Resource Marketing Inc.'s management's assertion for the period January 1, 1998 through February 28, 1999 is fairly stated, in all material respects, in conformity with the AICPA/CICA WebTrust Criteria.

The CPA WebTrust seal of assurance on Resource Marketing Inc.'s Web site for electronic commerce constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of Resource Marketing, Inc's services nor their suitability for any customer's intended purpose.

Fleming, Brockschmidt & Durkin PLL

Certified Public Accountants

Cincinnati, Ohio
March 1, 1999

# Disclosure of Business Practices

1. **What is your policy regarding customer privacy?**

   We never provide any other parties with access to your email address, postal address, or any other information that we may collect from you.

2. **Do you use cookies, and do you store any information on my machine?**

   Resource Marketing uses no cookies and stores no information on your machine in the electronic commerce process.

3. **What is the average time from the placement of my order to the delivery of an order?**

   **TradeBanner** member registrations, **TradeBanner** advertising purchases, **Web Hosting** and **Dialup Services** applications are generally processed within 2 business days.

4. **What are your payment terms for TradeBanner registration and TradeBanner advertising purchases?**

   **TradeBanners** services need payment in full by credit card or check before services are rendered.

5. **What fees are due to initiate Web Hosting or Dialup services?**

   Setup fees, the current month's prorated fees, and the next month's monthly charges are due when your order is placed.

6. **How will I be billed for monthly Web Hosting or Dialup charges?**

   Monthly charges are billed in advance. We will charge your credit card on the first of every month for that month's services. Payments made by check are due no later than the 10th of the month.

7. **Will the customer be informed of problems with a delivery and their options?**

   We will contact you as soon as we know your order will be delayed. The only reason your order could be delayed is if your credit card is declined or your check is returned, in which case we will contact you immediately for another card number or to make other payment arrangements.

8. **How are the items normally delivered?**

   **TradeBanners**: Banners over the Internet, password and account numbers emailed.

   **Web Hosting**: Usernames and passwords via email.

   **Dialup Services**: Within the greater Cincinnati, Ohio area you can have software installed on

your computer and receive training by one of our technicians for a flat fee of $95.00 at your location. Outside Cincinnati we fax, phone, or email your account names and passwords.

9. **Are there any charges related to ordering electronically?**

   No. No additional fees are charged when placing an order electronically.

10. **How may services be cancelled?**

    **TradeBanners**: Once your order is initially processed, your order cannot be cancelled.

    **Web Hosting**: Once your order is processed, your web hosting agreement can be cancelled upon 30 days written notice. You will be liable for services rendered during those 30 days.

    **Dialup Services**: Once your order is processed, your dialup service can be cancelled upon 30 days written notice. You will be liable for services rendered during those 30 days.

11. **Are there any other terms applicable?**

    ADDITIONAL TERMS AND CONDITIONS:

    A late payment charge of 1.5% per month is due on overdue accounts. If a customer fails to make payment in full when due, customer shall be responsible for all collection costs incurred by Resource Marketing, Inc. including attorneys' fees and court costs.

12. **If I have a question or complaint, where can I mail it?**

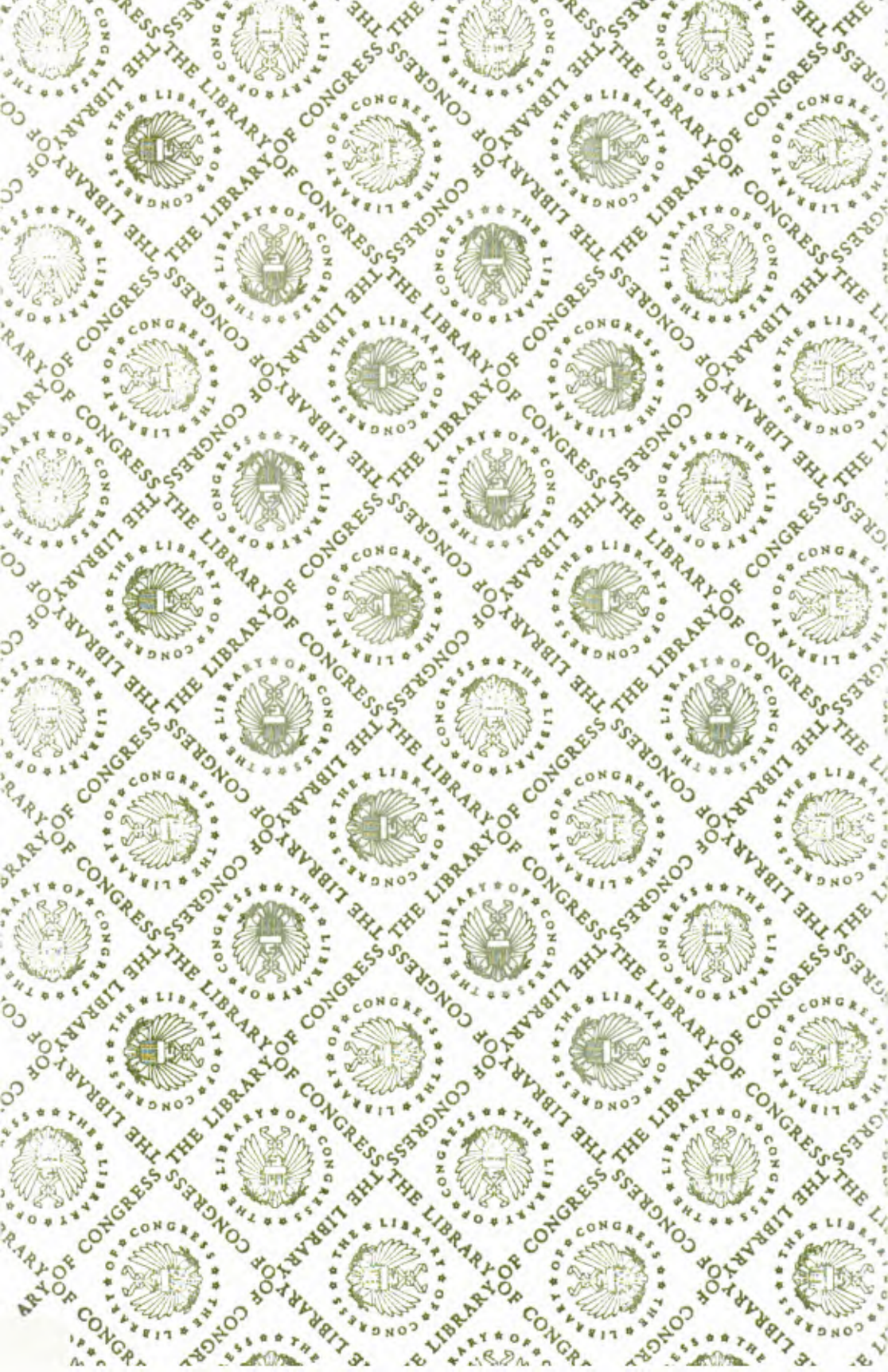
    Resource Marketing, Inc.
    61 Covert Place
    Ft. Thomas, KY 41075

13. **Is there a phone number where I can reach an employee?**

    For customer service and other information contact us at (606) 441-8700, Monday through Friday, 9am to 5pm EST. Any calls placed outside those hours will be transferred to our voice mail system and will be returned the next business day. Calls during this period reaching a busy signal will be routed to a voice mail system checked multiple times daily. We also are available 7 days a week via e-mail at help@resource-marketing.com, and try to return email within the 2nd business day.



ISBN 0-16-060799-X


THE LIBRARY OF CONGRESS